Network Control and Management Architectural Framework Supporting Military Quality of Service

Marek Kwiatkowski

DSTO-TR-0871

19991027 111

Network Control and Management Architectural Framework Supporting Military Quality of Service

Marek Kwiatkowski

Communications Division
Electronics and Surveillance Research Laboratory

DSTO-TR-0871

ABSTRACT

The growing demand for multimedia/multiparty services and their rapid design, deployment and modification using cell/packet infrustructure is apparent in the ADF. A well-chosen uniform Military Network Control and Management (M-NC&M) architecture covering both strategic and tactical domains may have an enormous impact on achieving these goals. This report proposes a general framework for such an architecture, in the medium term (5-10 years). The proposed framework follows concepts of an open and programmable network environment, and adds to them military specifics pertinent to the ADF. A particular emphasis of the framework is put on the way the military aspects of Quality of Service should be supported by the M-NC&M.

RELEASE LIMITATION

Approved for public release

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION **DSTO**

DTIC QUALITY INSPECTED 4

Network Control and Management Architectural Framework Supporting Military Quality of Service

Executive Summary

The growing demand for multimedia/multiparty services and their rapid design, deployment and modification is apparent in the ADF. To fulfil this requirement a high bandwidth (i.e. hundreds of Mbit/s) fixed core network with medium bandwidth (i.e. tens of Mbit/s) mostly satellite links to the tactical domain are being built. Packet/cell switching technologies will be used in this interconnected environment due to their more flexible bandwidth allocation, simpler control and better adaptability to bursty traffic than circuit switching counterparts.

To achieve good prediction of multimedia service behaviour, end-to-end Quality of Service (QoS) guarantees through all crossed networks must be supported. In addition, in military networks, when not enough capacity is available to send all information (e.g. due to congestion in impoverished links, partially destroyed networking infrastructure, jamming), messages carrying mission critical information should be delivered first. Unfortunately, today's packet/cell based ADF networks do not enable traffic prioritisation based on its military importance.

A well-chosen uniform Military Network Control and Management (M-NC&M) architecture covering both strategic and tactical domains may have an enormous impact on:

- Ability to support end-to-end QoS;
- Ease of designing, deploying and modifying new services across all interconnected assets;
- Efficient use, from the military viewpoint, of these assets in stressed (overloaded) situations;
- Smooth evolution of legacy capabilities;
- Reduction in complexity.

The aim of this report is to propose a general framework for such an architecture. It focuses on packet/cell switching technologies in the strategic communication infrastructure and its interconnection to the tactical domain. The report refers to medium term (5-10 years) design goals.

The report assumes that Defence will manage switches/routers involved in passing military traffic. Any commercial carriers' involvement in transmission services between these switches/routers will be through permanent or semi-permanent paths set-up using management systems of the carriers. Each carrier will guarantee QoS of their transmission services.

In the first part of the report the requirements for the proposed M-NC&M architecture are specified and a review of standardised network control and management architectures, both currently used and being developed, is given. The most important findings of this part are:

(1) In the military environment, QoS should be managed as a function of its military value. This approach is referred to as delivering Military QoS (M-QoS). Greater resilience of mission-critical flows during overloads can be achieved using this approach;

(2) There are strong arguments to gradually "step down" in QoS of less important military flows in overloaded networks, instead of releasing these flows;

(3) The M-NC&M architecture should be as transparent as possible to the used transmission infrastructure since no single winning transportation technology for multimedia/multiparty networks is expected in the commercial world for the foreseeable future;

(4) Traditional Network Control and Management systems such as Signalling System No 7 (SS7), Telecommunication Management Network (TMN) and the Internet cannot support rapid designing, deploying and modifying of multimedia services, prioritisation of information flows according to their military value, or enabling graceful degradation of QoS. A solution to achieve these requirements is to create an open and programmable network environment. The term *open* means that standard *Application Procedure Interfaces* (APIs) are used to access network elements (e.g. routers, ATM switches) and basic network services. The term *programmable* refers to flexibility achieved by using high level languages to (a) represent functionality of network resources by a set of software abstractions; and (b) access (manipulate), through APIs, capabilities of these resources.

Considering these findings an M-NC&M architectural framework is proposed in the second part of the report. This framework follows concepts of an open and programmable network environment developed by TINA, XRM and IEEE P1520 standard initiatives, and adds to them military specifics pertinent for ADF networks. A particular emphasis of the framework is put on the way M-QoS should be supported by the M-NC&M. A case study is also presented showing the applicability of this framework to an ATM environment.

The report recommends that DSTO should:

• Improve liaison with Defence Information Systems Group (DISG), especially the Network Operations Centre and the Network Technical Services at Deakin, ACT;

• Find detailed mechanisms to fulfil requirements posed to the M-NC&M. Regarding studies on mechanisms improving network robustness and performance, close collaboration should be established with Drs Miro Kraetzl and Peter Shoubridge, Communications Division, DSTO, to utilise their expertise in network performance and survivability;

- Specify a standardised software interface between user applications being built by DSTO and the experimental M-NC&M implemented on the EXC³ITE network;

- Launch a study to analyse distribution of service management algorithms for user applications implemented in ADF networks;

- Launch a study to analyse scalability and performance of M-NC&M mechanisms;

- Intensify experiments on the use of available commercial and experimental software to gain practical experience in building various M-NC&M mechanisms;

- Constantly monitor new developments in research on open and programmable networks;

- Establish liaisons with the COMET group at Columbia University, one of the most active groups conducting advanced research on open and programmable networks;

- Establish liaisons with the US Air Force Laboratory at Rome, NY, the leading US Defence research unit working on military network management. The aim is to exchange information about M-NC&M architecture(s) that are currently used and planned to be used in US Defence networks.

Authors

Dr Marek Kwiatkowski
Communications Division

Dr Marek Kwiatkowski received the M.Sc. degree from the Silesian Technical University, Gliwice, Poland, in 1979 (Computer Science), and the Ph.D. degree from AGH, Cracow, Poland, in 1990 (Telecommunications). From 1991 until 1998, he worked at the Teletraffic Research Centre, University of Adelaide, first as a Post Doctoral Fellow, and from 1995 as a Research Fellow. Since June 1998 he has been working at the DSTO, Network Integration Group, as a Senior Research Scientist. His main research interests include control and management aspects of multimedia military and commercial networks.

Contents

1. Introduction

In the 1997 *Australia's Strategic Policy* (ASP 97) document the revolution in military affairs is perceived as closely linked to the information revolution, which in turn is changing the nature of warfare all over the world [FLAH98]. The same document recognises that the ability to get information **to the right place at the right time** is the critical requirement for effective Command Arrangements and Command Support Systems. Military telecommunications networks are clearly vital links in delivering this information, and their *control and management* (NC&M)[1]systems are responsible for fulfilling the above requirement.

Due to recent advances in transmission and processing technologies, commercial networks are undergoing an explosive growth of new multimedia/multiparty services, (such as video conferencing and collaborative distributed environment) with a broad range of Quality of Service (QoS) requirements. In addition, developments in distributed systems and transportable software (e.g. CORBA, Java) facilitate creating such services. However, the essential issue in this process is to make currently used networks *open* and *programmable* (as opposed to traditional hermetic and rigid approaches), so that services creation, deployment and modification can be rapid and relatively easy. Additionally, reduction of complexity is a major feature of open systems, particularly in heterogenous environment, due to the use of standardised (i.e. common) programmable interfaces.

Demand for multimedia/multiparty services and their rapid design, deployment and modification is visible in ADF as well. One of the goals described in Annex E of a draft *Defence Information Environment Strategic Plan 2010* is to: *"Develop deployable and fixed communications system, including messaging, voice, facsimile, video and electronic information exchange"*. To make it happen, the primary requirement is to offer to ADF customers sufficient amount of bandwidth both in strategic and tactical environments.

To fulfil this requirement the ADF's strategic telecommunications infrastructure is currently undergoing major changes, namely:

- Circuit switching networks are being replaced by high bandwidth (i.e. hundreds of Mbit/s) packet/cell switching technologies due to their more flexible bandwidth allocation, simpler control and better adaptability to bursty traffic than circuit switching counterparts.

- ADF's terrestrial packet based WANs (offering, for example X-25, Frame Relay services) and (mainly IP-based) LANs, developed over the past decade as separate entities, are gradually interconnected by a corporate (strategic) backbone broadband infrastructure (DSDN).

---

[1] The distinction between control and management refers to different time scales, that is, *control* mechanisms operate in near real-time, while *management* ones refer to longer intervals.

It is stressed that the strategic Defence infrastructure uses commercial carriers' permanent or semi-permanent paths (e.g. SDH, ISDN links) between switches/routers is a typical solution to cut costs. The set-up of these paths is performed using management systems of the carriers.

During the next several years, ADF plans to improve currently impoverished tactical communications infrastructure and its interconnection with the strategic one using commercial assets. The following changes are expected:

- Launching in year 2000 the Optus C1/D satellite;

- Obtaining access to *Personal Communications Services* (PCS) networks, such as IRIDIUM;

- Deployment of Military GSM (MGSM).

The above listed changes will soon create an interconnected high bandwidth core military infrastructure with medium bandwidth (i.e. tens of Mbit/s) links to the tactical domain. This infrastructure will enable deployment of many new sophisticated multimedia/multiparty services. However, as for the commercial networks, to achieve good prediction of service behaviour, end-to-end QoS guarantees through all crossed networks must be delivered using NC&M mechanisms.

On the other hand, in military networks, when not enough capacity is available to send all information "at the right time" (e.g. due to congestion in impoverished links, partially destroyed networking infrastructure), messages carrying vital (from the military viewpoint) information should be delivered first. Unfortunately, today's packet/cell based ADF networks do not enable traffic prioritisation basing on its military importance.

A well-chosen uniform *Military Network Control and Management* (M-NC&M) architecture covering both the strategic domain and its extensions to the tactical domain may have an enormous impact on:

- Ability to support end-to-end QoS;

- Ease of designing, deploying and modifying new services across all interconnected assets;

- Efficient, from the military viewpoint, use of these assets in stressed (overloaded) situations (i.e. achieving high survivability with maximum performance) ;

- Smooth evolution of legacy capabilities;

- Reduction in complexity.

The aim of this report is to propose a general framework for this architecture. The report refers to medium term (5-10 years) design goals. It focuses on packet/cell switching technologies in the strategic communication infrastructure and its interconnections to the tactical domain. The report assumes that switches/routers

involved in passing military traffic will be managed by Defence. Any commercial carriers' involvement in transmission services between these switches/routers will be through permanent or semi-permanent paths set-up using management systems of the carriers. Each carrier will guarantee QoS of their transmission services. If it cannot be assured by a carrier, an appropriate notification will be sent from the carrier to the military network using standard management interfaces. Any Defence requirements regarding setting-up or changing transmission characteristics will also be exchanged through these interfaces.

The structure of the report is as follows. In Section 2, the requirements for the proposed M-NC&M architecture are specified. A brief review of standardised network control and management architectures, both currently used and being developed is given in Section 3. Basic features of the proposed architecture and the way it covers requirements posed in Section 2 are described in Section 4. In Section 5, a case study is presented showing the applicability of this framework to an ATM environment. The research problems that remain to be solved are outlined in Section 6.

2. Requirements for the Architecture

It is essential that the future Military Network Control and Management (M-NC&M) architecture should:

1. *Perform traditional management functions;*
2. *Support military QoS;*
3. *Enable graceful degradation of QoS in overloaded conditions;*
4. *Cover heterogenous networks;*
5. *Be secure;*
6. *Support deployment of multimedia/multiparty applications;*
7. *Enable rapid design and deployment as well as modification of new services;*
8. *Be robust to failures and changing environment;*
9. *Have high performance;*
10. *Have good scalability;*
11. *Use of industry standards.*

Below, the above goals are explained in detail.

2.1 Traditional Management Functions

Following the ISO OSI standards (also adopted by ITU), traditional network management activities performed by M-NC&M are:

*   *Configuration management*, providing functions to control, identify and collect data from and provide data to network elements;
*   *Fault management*, enabling detection, isolation and correction of abnormal operation;
*   *Performance management*, used to evaluate and report upon behaviour of telecommunications equipment and effectiveness of the network;
*   *Accounting management*, enabling the use of a network service to be measured and the costs for such use to be determined;
*   *Security management* used to control the integrity, confidentiality, and continuity of network services against security threats.

2.2 Military QoS

Currently emerging and future distributed multimedia public networks will carry traffic such as video, audio and computer data with a broad range of QoS requirements, usually in terms of delay, jitter and error rate. Meeting QoS guarantees is fundamentally an end-to-end issue that is from application-to-application [AURR98].

Supporting end-to-end QoS guarantees (i.e. through all crossed networks) means **better prediction of service behaviour**. To achieve this, end-to-end admission testing and resource reservation has to be done before flow of media information commences, along with active monitoring and maintenance of the delivered QoS while the flow is pending.

In the military environment, delivering end-to-end QoS guarantees is even more crucial. In stressed (overload) situations, the "best effort" policy (e.g. currently used in Internet) may lead to unacceptable delays jeopardising whole missions. It should be noted that simple adding transmission capacities to links and more processing power to network nodes to cope with the load does not solve the problem. This is because the network should be able to efficiently perform and attempt to maintain QoS in stressed situations when only a part of all resources may be available. It is also expected that the increase of transmission capacity to currently impoverished satellite links between strategic and tactical networks will be much slower than inside ADF's strategic, mostly fibre optic networks. Therefore, the delivery of QoS to satellite networks is of great importance.

On the other hand, in the military environment there are strong arguments to manage QoS as a function of its *military value* (e.g see [KOWA96b, KOWA98c]). In [PORE98], preemption of ATM connections based on mission priorities is considered. Maximum number of preemptions for a new call is assumed. Preemption of traffic flows as a function of their military value is analysed in [KOWA96b] and [BLAC98]. We propose that the military value to be expressed by the following factors:

- *Mission priority* set by a commander;
- *User's rated own contribution*, for example high, medium, low;
- *Time relevance*, specifying what happens if information is not delivered on time;
- *Traffic type*, for example audio, video, data etc.

Note that the first three factors may change their values during the transfer of information.

Considering military value provides greater resilience of mission-critical flows during overloads. A typical mechanism that can be used for this purpose is *prioritisation* of information flows. We will call this approach *delivering Military QoS (M-QoS)*, and we perceive this as a strong requirement for the M-NC&M architecture to support. Since the military value of a flow may change with time [KOWA96a, BLACK98], M-NC&M

5

should have mechanisms (e.g. prioritisation/preemption) reflecting in real-time such changes.

Note also that the prioritisation based on military value being a function of the above factors has already been successfully implemented in the *Australian Theatre Broadcast System* (TBS), which is a trial capability under JP 2008 [STIM99]. In this system, a number of "logical channels" is set up, each competing for bandwidth in the same satellite physical channel. An intelligent scheduler has been designed at Communications Division, DSTO, to dynamically allocate the available bandwidth maximising total military value delivered over a TBS (see [BLAC98] for details)

It is stressed that some traffic not related to any particular missions and flowing across the interconnected ADF networks may not require M-QoS support. An example might be the traffic produced when using the World Wide Web for entertainment purposes. M-NC&M should offer to this traffic the best-effort service.

2.3 Graceful Degradation of QoS

In the military environment appears a problem of how Network Control and Management should react, when there are not enough resources to establish/maintain important flows. *Should less important ones be released, or rather maintained but with the lower QoS?* The former approach is proposed in [PORE98], where for an ATM military network an algorithm for connection prioritisation/preemption is considered. The author assumes that if a more important connection pre-empts a less important one, the latter should be released. Clearly, this approach is simple to implement.

However, we advocate using gradual "stepping" down in QoS mainly due to the following reasons:

1. If a connection is deleted (instead of maybe slowing it down), it is impossible for many types of applications to resume the transfer from the point it was stopped. Consequently, such applications need to retransmit the whole transfer from the beginning.

2. In some instances, constant attempts of re-establishing connections after their deletion may cause an avalanche of control messages deteriorating congestion situation even further.

When degradation of QoS happens, the end user may decide to (a) maintain the session; (b) choose a service requiring less transmission bandwidth; or (c) quit. Moreover, if (a) is chosen, and if the reason for the QoS deterioration disappears, the QoS can be immediately restored.

2.4 Covering Heterogenous Environments and Networks

In the past, the ADF communication environment was composed of a set of separated fixed and satellite heterogenous networks used to communicate both in strategic and tactical domains. A strong tendency to integrate these networks is visible nowadays. A wide range of routers, switches and host systems (from portable to high performance workstations) is connected to these networks. To achieve seamless connectivity of this strategic-tactical network, the M-NC&M will have to cover diverse environments, namely:

- *Fixed networks.*

  These networks will be used in the strategic domain in form of the core Wide Area Network (WAN) connecting islands of Local Area Networks (LANs) as well as Metropolitan Area Networks (MANs), for example installed in military bases. It is expected that fixed networks will deliver medium to high connection rates ranging from single to hundreds of Mb/s.

- *Wireless/mobile networks* (both terrestrial and satellite).

  It is expected that wireless/mobile networks will deliver transmission rates between tens of kb/s to tens of Mb/s. These networks will be deployed to:

  - Link strategic and tactical networks, as well as tactical networks between themselves - satellite connections will mainly be applied for this purpose;

  - Support communication within (movable) tactical networks - *Military GSM* (MGSM) and *Low Earth Orbit* (LEO) satellite systems (e.g. IRIDIUM), supporting Personal Communication Services (PCS), as well as *Wireless Local Area Networks* (WLANs) are most likely technologies to be used.

During the time frame considered in this report (next 5-10 years), the following two factors are expected to play a particularly important role in these changes:

- Trends in commercial telecommunications;

- Trends in (technologically more advanced) US Defence which is the ADF's major ally.

Below, we discuss some probable scenarios for changes in the commercial world and US Defence in relation to fixed, terrestrial wireless/mobile as well as satellite environments.

2.4.1 Fixed Networks

The current market of fixed networks is very chaotic, therefore it is extremely hard to predict its developments even during the next couple of years. However, several parallel trends are visible:

1. *ATM-only* solutions.

    ATM has not succeeded to be the ubiquitous broadband technology for both local and wide-area environments in a sufficiently economical manner, but it is a solid addition to the telecommunications market. It is noted that some carriers still seriously consider its use as a core technology up to the desktop computer. For example, Sprint, the third largest U.S. long-distance operator has recently announced plans to roll out an integrated, end-to-end managed ATM service aimed not only at corporate customers, but also at medium-sized enterprises and residential customers [BLAU98]. In addition, Sprint is working with Cisco to develop a customer premises device costing about $200, that will bring integrated ATM services to the home or enterprise. Internationally, Sprint, Deutsche Telekom, and France Telecom are planning to launch cross-border seamless ATM services within their Global One alliance by the end of 1998 [BLAU98]. Such developments in the market may lower prices of (currently expensive) ATM solutions.

2. *IP-only* solutions.

    The Internet, using *Internet Protocol* (IP) has demonstrated its capability to evolve to an enormous worldwide network by interconnecting a large number of heterogenous subnetworks and offering cheap connectivity to desktop computers. There are also large numbers of (cheap) TCP/IP and UDP/IP applications, including IP-telephony and multimedia applications.

    To cope with still faster growing traffic, carriers can use nowadays relatively cheap fibre-optic trunks and emerging (but expensive) gigabit routers. However, the best-effort approach of IP (i.e. without reserving any network resources) is not sufficient for QoS sensitive real-time multimedia applications even under medium network loads. Although the *Internet Engineering Task Force* (IETF) has set up several initiatives to resolve this problem (e.g. using reservation protocols), no one has been yet unanimously received by the commercial world.

    Hoping the problem of IP QoS will somehow be solved, some carriers, such as recently allied BT and AT&T, are considering the creation of networks with IP directly mapped to SDH or (later) to the *Wavelength Division Multiplexing* (WDM) infrastructure.

3. *IP over ATM* solutions.

    Although ATM is still an expensive technology and imposes overheads, many experts believe that combining the flexibility of IP routing at the Network Layer

with good scalability and fast-switching capability of ATM is a viable solution. There have been a number of approaches proposed by such bodies as the IETF and the ATM Forum. Difficulties in mapping IP to ATM have been a significant driver in the development of a number of proprietary label switching technologies (e.g. IP switching, Cell Switching Router, Tag Switching, Aggregate Route-based IP switching, IP Navigator). What differentiates them is their use of label swapping techniques, IP control protocols and label distribution mechanisms. Standardisation is currently ongoing to achieve a non-proprietary approach. Naturally, multimedia applications such as (usually long lasting) video conferencing can greatly benefit from this solution. In addition, the QoS capabilities inherent in ATM are utilised.

As far as trends in US Defence fixed networks are concerned, ATM is expected to be a key transport technology of the National Information Infrastructure and the information infrastructure of the Department of Defence for supporting voice, video, data and multimedia services [VAKI98, HADJ98, SHVO98, ELMO98]. Therefore, ATM will also be the preferred technology for *Command, Control, Communications, Computer and Intelligence* (C4I) systems [BOWM98].

2.4.2 Terrestrial Wireless/Mobile Networks

Nowadays, terrestrial wireless/mobile networks are mainly used for voice communications due to transmission rate limitations. However, rapidly growing interest in using radio systems for Internet access and even for multimedia services has caused an extensive research and standardisation efforts to enable delivery of considerably higher rates.

In the case of wide-area (metropolitan) systems, such as GSM, peak data rates will soon range from 10-100 kb/s. Using microcell technologies, delivery of data services in the 30-500 kb/s range is feasible. Rates of 2 Mb/s in a localised environment (i.e. microcells and in-building) and 150 kb/s in larger cells are expected to be available in a couple of years using standards such as the European *Universal Mobile Telecommunications Systems* (UMTS) and ITU International Mobile Telecommunications in year 2000 (IMT-2000) [CIMI98]. Wireless Local Area Networks (WLANs), already available for several years and delivering speeds up to 2 Mb/s, are expected to support rates up to 20 Mb/s using for example the HIPERLAN standard.

As far as transportation layers are concerned, similar trends to those of fixed networks are visible in mobile/wireless ones, namely:

- *Wireless/mobile IP.*

  Mobile IPv4 is a relatively new standard proposed by the IETF to support mobile users. It allows a mobile computer to be reachable using the same IP address regardless of its current point of attachment to the Internet. However, unlike fixed networks, wireless ones are characterised by lower bandwidth and are prone to losses due to interference. In these conditions, delivering guaranteed QoS is of even

higher importance than for fixed counterparts. Unfortunately, Mobile IPv4 does not offer this feature.

- *Wireless/mobile ATM.*

  Wireless/mobile ATM intends to extend all the benefits of the fixed environment with delivering QoS. There are extensive standardisation efforts within the ATM Forum to provide wireless/mobile ATM extensions to fixed ATM networks, with fully accepted specification planned for 1999. A separate, already advanced research project in this area has been initiated by the COMET Group at Columbia University. This group has created a software middleware platform called *Mobiware* that seamlessly runs on mobile devices, base stations and mobile-capable ATM switches [CAMP96]. Delivering QoS guarantees in mobile environments is particularly challenging due to mobility requirements, limited radio resources and fluctuating network conditions. ATM can successfully be implemented in wireless LANs, as for example described in [DU98].

  It is noted that since wide-area wireless communication is characterised by limited capacities, overheads due to a header in each (small size) ATM cell have a more detrimental effect than for fixed (high-capacity) ATM networks.

- *IP over wireless/mobile ATM.*

  There are two basic approaches supporting IP over wireless/mobile ATM [ACHA98]. In the first one, the ATM signalling is extended to enable location management and handovers. IP is mapped to mobile ATM, which hides mobility aspects from IP. In the second approach, the IP stack is directly executed over ATM switches, and Mobile IP (see above) is utilised to route packets to a mobile terminal's current location.

In the US Defence, the use of packet/cell transmission modes in (terrestrial) wireless/mobile military environment is not yet matured. There is an initiative to create *Wireless/Mobile ATM* (WATM) extension to the *Defence Information Systems Network* (DISN), which is an ATM based fixed network [SHAH98]. The main goal is to provide warfighters with location independent and high capacity (approx. 20 Mb/s) access to broadband networks. Both pure ATM and IP over ATM multiparty/multimedia applications with QoS guarantees are planned. The use of Mobile IP over ATM is also assumed in this approach. A proposal for applying Mobile IPv4 with no QoS guarantees in the tactical military architecture is presented in [GRAF98].

2.4.3 Satellite Networks

Satellites are mainly utilised for voice communications and TV broadcasting. However, there are already existing products, such as Comsat ALA-2000 or Yurie LDR200 (e.g. see [WILK97]), in the market using satellite links for packet/cell transmission.

Satellite ATM technology potentially can offer users all the benefits of terrestrial ATM networks, including multiparty/multimedia services with QoS guarantees. However, several obstacles have to be overcome to enable this technology to be used in full. These include a need to define a satellite-specific MAC-sublayer, a fast and efficient conversion protocol improving performance between LANs/MANs and ATM satellite connections, as well as mechanisms minimising delay for real-time applications [AKIL97]. Since satellite ATM connections can offer considerably higher rates than wide-area terrestrial wireless/mobile communication, the impact of overheads due to the presence of ATM headers is not that severe for the former connection types as for the latter ones.

IP-type communication can be directly implemented in satellite channels but thus far, it does not offer QoS guarantees. However, as shown in [BLAC98], if applications using a single satellite channel can specify QoS or M-QoS requirements, applying a task schedular in the source node of a satellite connection can deliver QoS or M-QoS, respectively.

It is stressed that the use of TCP over IP in the satellite environment is very inefficient due to the error-control mechanisms optimised for terrestrial (small latency) networks. To overcome this problem, the satellite segment of a TCP connection can use a different protocol, optimised for this type of communication. Examples of such an approach can be found in [STAD98].

In the US Defence, the ATM technology is mainly used for packet/cell transmission modes in satellite communication. The use of the TCP/IP protocol suite over a single channel of a geostationary satellite is described in [STAD98]. This approach, being sponsored by the Department of the Air Force, can be utilised for transmission of Internet data via satellite but without QoS guarantees.

2.4.4 Implications for M-NC&M

The arguments presented in previous sections show that there might be no winning packet/cell transmission technology for the foreseeable future, and all of the above discussed solutions may be potentially used in ADF networks for a long time. Therefore, M-NC&M should be designed for seamless delivery of end-to-end connectivity over different transmission protocol stacks.

2.5 Security

Security of management is of extreme importance in Defence networks, so M-NC&M should sufficiently support it. This type of security deals with various threats, including viruses, attempts to steal/misuse network management information, attacks on network installations, which can be catastrophic. Typical services that protect the network against such threats include [AIDA98]:

- *Peer entity authentication,* establishing the identity of the initiator of the operation;

- *Data origin authentication,* assuring that data really comes from the source where they seem to;

- *Connectionless integrity,* guaranteeing that protocol data units (PDUs) carrying management information cannot be modified without detection ;

- *Stream integrity,* assuring that PDUs are not misplaced in a stream;

- *Confidentiality,* preventing capturing of management information;

- *Access control,* defining which objects are allowed to manage other objects.

2.6 Support of Multimedia/Multiparty Applications

It is anticipated that Defence networks, similarly to public ones, will have to carry all types of media traffic such as video, audio, imagery services and computer data with a diverse range of QoS requirements. Since multimedia applications, such as video conferencing and collaborative distributed environments are likely to be popular in the ADF, the integrated networking infrastructure will have to support:

- Point-to-point (unicast) connections;
- Multicast connections;
- Broadcast connections.

2.7 Deployment of New Services

Expected improvements in transmission and processing capabilities will enable to implement many new sophisticated services in ADF networks. Using recent developments in distributed software engineering, better modularity, re-useability, reliability and scalability can be achieved in comparison with the traditional function-oriented approach. An M-NC&M architecture should utilise these developments, so that new services can be rapidly designed and deployed as well as easily modified.

2.8 Robustness

Network control and management, being a vital part of every network, should be very robust to failures due to both natural causes and intrusion. In addition, in stressed situations the military environment is characterised by often changing transmission capabilities. M-NC&M should be able to quickly adapt to these changes and enable efficient utilisation of available assets. Therefore, military networks are expected to be dynamically reconfigurable. In addition, the performance of a network should gracefully deteriorate in case of a failure, so that it could transfer as much information as possible even in severely overloaded conditions. The M-NC&M architecture should support such graceful degradation.

It is stressed that to achieve robustness it is crucial for M-NM&C to be equipped with mechanisms for fast detection of changes in the network [SHOU99].

2.9 Performance

M-NC&M should be very efficient in the sense that vital control and management functions should be promptly performed both in case of low/medium loads as well as during overloads. The amount of control/management information should minimally affect the bandwidth available to users.

2.10 Scalability

The proposed architecture should be well scalable. That is, it should easily cope with the predicted (rapid) growth of both the amount of transferred information and the number of information flows in Defence networks during the time frame considered in this report.

2.11 Use of industry standards

Network control and management systems are very costly to develop, particularly software. Current Defence cost reduction strategy is to deploy the most current *Commercial-Off-The-Shelf* (COTS) products with minimal development costs. This approach should certainly be used when developing M-NC&M. Two stages of this development can be distinguished:

1. Choosing appropriate commercial software tools available in the market.

   Since network control and management systems are planned to perform for a long time, these tools should be based on (stable) industry approved standards. Using proprietary solutions not supported by standards is too risky from the long-time perspective, and makes it difficult to interwork with commercial carriers and allied networks.

2. Using software described in (1) to develop a control and management platform that satisfies ADF requirements.

3. Review of Network Control and Management Architectures

A brief review of standardised network control and management architectures, both currently used and being developed is given in this section. We start by presenting traditional approaches and argue that some crucial requirements listed in Section 2 cannot be fulfilled by these architectures. Then we describe several newly developed network control and management architectures, which enable the drawbacks of the traditional architectures to be overcome.

3.1 Traditional Approaches to Network Control and Management

3.1.1 The ITU Approach

The ITU approach to network control and management in telecommunication networks is based on using two separate building blocks:

- *Signalling System Number 7 (SS7)*;

  The SS7 is used both in the narrowband ISDN (ITU standard Q.931) and in broadband ATM networks (ITU standard Q.2931). The functioning of SS7 relies on the existence of two standard interfaces:

  - *User Network Interface* (UNI); and

  - *Network Node Interface* (NNI).

  This model, originating in early 70's, has been successful in delivering reliable basic telephone services and value-added enhancements by use of *Intelligent Network* (IN) services. The SS7 with an additional part called *Mobile Application Part* (MAP) is also used in wireless/mobile networks such as GSM. The use of the same signalling system in both fixed and wireless/mobile networks facilitates their integration.

  The major assumption behind the SS7 model was that customers use dumb terminals and only a network can offer "intelligence" by means of *Service Control Points* (SCPs).

- *Telecommunications Management Network* (TMN).

  The OSI based TMN is a conceptual and technological framework that offers:

  - A set of *standardised interfaces*, designed to transfer management information between a TMN, being a conceptually separate subnetwork, and

telecommunications network equipment, as well as between TMNs of cooperating networks;

- An object-oriented architecture, in which the physical and logical resources of a telecommunications network are viewed as objects that can be managed. The *Management Information Base* (MIB) is used as a repository of management objects;

- An *organisational model* using the *manager-agent* concept, where an agent accomplishes management operations on managed objects according to directives obtained from a manager, and returns results of those operations in the form of notifications.

- A management layer model, that supports the complex task of managing by splitting this task into different functions and placing withing the following layers:

    - The *Network Element Layer*, responsible for the management of particular *Network Elements* (NEs);

    - The *Network Element Management Layer*, used to control and coordinate groups of NEs;

    - The *Network Management Layer* performs control and coordination functions for all NEs which belong to the same carrier;

    - The *Service Management Layer*, involved in the control and management of services as well as in the interactions with service providers and customers subscribing services;

    - The *Business Management Layer*, which manages business aspects of the whole network.

- A *communication model*, that describes the functions, protocols and messages involved in exchange of information between TMN entities. The OSI protocol stack is used, with *Common Management Information Protocol* (CMIP) and *File Transfer Access and Management Protocol* (FTAM) being at the Application Layer. CMIP is a transaction-oriented protocol capable of invoking a reach set of operations on managed objects. It enables creating both centralised and hierarchical management systems.

Regarding requirements for M-NC&M listed in Section 2, the ITU approach has the following features:

1. *Covering traditional management functions.*

    These functions are well supported by TMN. A number of generic management functions are standardised creating a well-defined framework for dealing with common tasks and achieving reusability [AIDA98].

2. *Military QoS and its graceful degradation.*

   The ITU approach uses QoS service classes, each specifying which network performance parameters are relevant and to what values. A concept of an *ATM Transfer Capability* (ATC) has been devised to specify the ATM-layer parameters and the applicable procedures. The ITU approach however, neither allows for specifying military QoS requirements nor enables to achieve graceful degradation of QoS. This is because current signalling standards with their hard-coded algorithms inhibit programmability and extensibility necessary to manipulate information flows according to the military requirements.

3. *Covering heterogenous environments and networks.*

   The ITU approach supports narrowband PSTN and (broadband) ATM networks as well as narrowband terrestrial wireless/mobile networks. It covers neither IP networks nor ATM interworking with IP networks, although there is ongoing work within the ITU to complete a specification for the latter [LUET98].

4. *Security.*

   Until recently, only a modest degree of security could be achieved using TMN. It mainly allowed changing passwords, usually transferred in the clear [JOHA96]. However, there are new standardisation efforts to enhance TMN standards with the specification of security mechanisms, security transformation techniques (including evaluation of *Generic Upper Layer Security* (GULS) for TMN purposes) and management of security.

5. *Support of multimedia/multiparty applications.*

   The ITU approach supports multimedia applications, but there is lack of flexibility in designing multiparty calls.

6. *Deployment of new services.*

   In case of SS7, the deployment of new services is very rigid and time consuming (taking up to years). Lack of service management infrastructure leads to a very limited third-party involvement in services programming. The network operator has almost complete control over designing and implementing new services. Moreover, only a small number of operational parameters are usually customised. Such approaches were sufficient (and efficient) for simple, audio-only, two-party applications, but certainly not future sophisticated multimedia/multiparty ones.

   TMN, being designed to manage a large number of simple objects, is not well suited for service management [KONG96]. To resolve this problem there are currently many attempts to integrate TMN network management with distributed processing environments such as CORBA (e.g. see [RAHK97, PARK96, DITT96]).

7. *Robustness.*

Both TMN and SS7 are mature and relatively robust technologies, but with some important limitations. The SS7 protocol stack is well protected against both transmission errors and congestion. On the other hand, a very complicated UNI signalling code is required for each terminal and switch. This feature can potentially be a source of failures.

TMN uses the connection-oriented CMIP protocol stack designed to cope with erroneous environments and loses of management messages. However, TMN, assuming a simple manager-agent relationship (a concept dating back mid-1980s), is not well suited to manage highly distributed (thus more robust) and dynamically reconfigurable networks [MART97]. In addition, adaptation of TMN to a changing environment is rather limited due to its lack of location transparency, requiring a manager to know the location of an agent (e.g. host address). That is why the ITU (jointly with ISO) has decided to extend the TMN model to include fully distributed management. This approach called generic *Reference Model of Open Distributed Processing* (RM-ODP) is being utilised by the TINA project aiming at replacing the traditional ITU network control and management by a fully distributed architecture (see the next section).

8. *Performance.*

The performance of the SS7 protocol stack is not very good resulting in long call set-up [OLIV98]. This is mainly due to the sequential, hop-by-hop connection establishment. Note that new multimedia calls require almost instant set-up times. The performance of TMN is satisfactory even for big networks. It can promptly react to network events due to the event-driven management (i.e. it does not require polling of network elements to obtain their status).

9. *Scalability.*

SS7 is well scalable and proved this feature while being implemented in narrowband networks. TMN is also well scalable by utilising hierarchical management and event-driven management.

10. *Use of industry standards.*

Both SS7 and TMN are very mature and well standardized concepts. Nowadays the commercial world offers many tool kits supporting TMN operation, for instance Hewlett-Packard's *OpenView* DM, IBM's *TMN WorkBench,* or DEC's *TeMIP,* just to mention a few.

3.1.2 The Internet Approach

As opposed to the ITU approach, the Internet technology relies largely on intelligence in user terminals. In the Internet, there is no strict distinction between network provider, service provider and user. Any user can be a service provider and network provider. This has been one of the most important features causing the enormous growth of this network. The Internet uses services of the connection-less Network Layer Internet Protocol (IP). No signalling (i.e. control mechanisms) inside the IP network is required since there are no network resource reservations for information flows. If Internet applications are sensitive to packet loses, they can use (above IP) the *Transmission Control Protocol* (TCP). This protocol uses retransmissions to cope with such loses. However, as mentioned in Section 2, the use of TCP in erroneous environments (e.g. satellite networks) is very inefficient since any losses are assumed be caused by congestion. Consequently, TCP slows the transmission rate to help the network to cope with the presumed overload. This even more aggravates the problem of delays in transferring of information.

The currently used IP Version 4 offers a *best-effort* service class. In this class, all packets are treated in the same way. Therefore, when congestion appears, no preferences are given to any packets. The best effort approach is not good enough for today's users. The growing demand for multimedia services has revealed the urgent need for the Internet to support QoS. That is why, during the last several years, the Internet Engineering Task Force (IETF) has proposed some solutions to cope with this problem, among which two have attracted much attention, namely:

- The *Integrated Services* architecture (Int-Serv) [INTS94].

  This architecture assumes that network elements (e.g. routers, subnetworks, end-user operating systems) offer services supporting QoS and appropriate interfaces through which those services are available. In addition to the best-effort service, Int-Serv offers the following new services [AURR98]:

  - *Controlled delay*, offering several standard delays to be chosen by a user;
  - *Predicated delay*, providing a statistical delay bound;
  - *Guaranteed delay*, which provides an absolute guaranteed delay bound.

  To deliver these services, Int-Serv recognises flows in a network that require QoS. These flows are characterised by (a) a *traffic specification*, describing traffic patterns pertinent to the flow; and (b) a *service request specification*, defining requested QoS.

  The *Resource Reservation Protocol* (RSVP) is used by Int-Serv architecture for end-to-end reservation of resources for QoS sensitive flows. This reservation, similar to traditional signalling, is performed at each router in the path between the source and destination. The RSVP is very well suited for multicast applications. It runs over both IPv4 and IPv6. It is likely that the Int-Serv approach will be at least implemented at the edges of enterprise networks, in user desktop computers. It is

already available on UNIX and LINUX platforms [RSVP98], as well as in Windows 98 and NT 5.0 [NORT98].

- The *Differentiated Services* architecture (Diff-Serv) [FERG97].

  This architecture has been proposed as a result of market pressure for immediate deployment of a QoS. In contrast to the per-flow orientation in Int-Serv, this architecture uses a small number of aggregated flows, based on the setting of bits in the TOS field of each packet's IP header. Diff-Serv focuses on aggregated flows thus diminishing the signalling traffic (i.e. there is no need to maintain soft states in routers). Application flows are aggregated to a limited set of class flows. Consensus has yet to be reached on the definition of these classes. The Diff-Serv is likely to be implemented in enterprise backbones [NORT98].

The network management in the Internet is composed of one or more *Network Management Stations* (NMSs) and one or more *Network Elements* (NEs). Like TMN, the Internet uses object orientation and manager-agent concepts. The managed objects are defined in the *Management Information Base* (MIB), which is different to the TMN MIB since objects in the Internet and those in OSI are different. The *Simple Network Management Protocol* (SNMP), a subset of CMIP, is used to transfer management information between an NMS and a NE. SNMP is a connection-less protocol and it has primarily been designed for environments with very low error rate, such as LANs and MANs. SNMP Version 1 (SNMPv1) only supports centralised management systems (i.e. a single NMS manages a set of NEs), and it does not allow for bulk transfer of management information. SNMP Version 2 (SNMPv2) additionally enables bulk transfers of management information (still rather poor comparing with CMIP) and offers structured management supporting manager-to-manager cooperation.

The M-NC&M requirements posed in Section 2 can be fulfilled by the Internet approach as follows:

1. *Covering traditional management functions.*

   SNMPv2 can provide all traditional management functions, but it is much less powerful in doing it than CMIP. Particularly, comparing with the latter, there are no sophisticated event facilities in SNMP and the information model is rather crude [AIDA98]. Additionally, the memory objects are static and cannot be instantiated.

2. *Military QoS and its graceful degradation.*

   The Int-Serv architecture sufficiently supports QoS. However, it allows for neither specifying M-QoS nor achieving graceful degradation of QoS because no such functions are available in RSVP. The use of the Diff-Serv architecture does not provide per-flow QoS but only on a per-class basis. Moreover, M-QoS and graceful degradation of QoS are also not supported.

3. *Covering heterogenous environments and networks.*

The Internet only supports IP-type networks. It can be used in all environments of interest, either being directly mapped to the *Medium Access Control* (MAC) Layer or using another underlying network (e.g. ATM). If Int-Serv is used, a better degree of interworking can be achieved between the Internet and ATM since both RSVP and ATM are connection-oriented. Although the majority of routers already supports Int-Serv, some of them may not, so it is necessary to determine what QoS management capabilities are available on the chosen communication path. The Diff-Serv model is also well suited to leverage off label switching technologies allowing IP to be switched by technologies such as ATM.

4. *Security.*

Security is poorly supported by both SNMPv1 and SNMPv2. It is expected that Version 3 (not yet standardised) will improve security by using authentication and access control [STAL98].

5. *Support of multimedia/multiparty applications.*

There are already available best-effort single-media protocols such as *Multicast Backbone* (Mbone) and *Real-Time Transport Protocol* (RTP) used as building blocks for applications. The same tool can be applied for different purposes by changing surrounding parameters. For example, the same audio tool can be used for both Internet telephony and Internet group collaboration. However, the control of such tools is currently rather limited and much work is required from IETF on scalable transport and signalling protocols to enable teleconferencing [CAMP97].

Int-Serv provides controlled QoS for multimedia applications. The way of specifying different QoS for separate end-points in multiparty applications needs further study.

6. *Deployment of new services.*

The deployment of new services is very easy since there are no technical barriers preventing any user to create and set-up its own service.

7. *Robustness.*

SNMP is less robust than CMIP used by the TMN because of it is connectionless mode of operation. In the erroneous environment, appropriate reliability of transferring management information can only be achieved by using retransmissions at the level of manager applications. On the other hand, SNMP is much simpler than CMIP, passing complexity to manager applications. Since SNMP uses the same manager-client model as TMN, its adaptation to changing environments is also rather limited.

8. *Performance.*

SNMP is particularly well suited for LAN and MAN environments that are connectionless, where the available bandwidth is high and the error rate very low [AIDA98]. If this is the case, the performance of SNMP is better than using CMIP. However, in wide area networks with substantial error rate and limited bandwidth (e.g. satellite networks), polling status of network elements and the need for retransmissions may result in noticeable additional load.

More research is needed to evaluate performance capabilities of RSVP, both in normal and overloaded situations.

9. *Scalability.*

SNMP has been designed to allow management of networks containing a very large number of network elements. SNMP scales very well if the managed environment is characterised by a very low error rate (e.g. LANs/MANs). Otherwise, performance problems may be encountered (see above).

If the Int-Serv architecture is used, it may suffer from scalability problems. This is mainly due to the need for all routers along the path to exchange significant amount of signalling messages, as well as to maintain per-flow state information. This information has to be periodically refreshed by the source. However, this problem may not be that severe in case of small and medium networks, such as ADF networks. Certainly, the Diff-Serv architecture poses less scalability problems.

10. *Use of industry standards.*

There is a plethora of tool kits supporting implementation of SNMP and design of its information model (including MIB). As for RSVP, it is already available on the majority of routers.

3.1.3 Summary

Although the traditional NC&M approaches satisfy some of the requirements listed in Section 2, some crucial ones are not supported. These include the possibility to cover heterogenous networks, implement M-QoS, achieving graceful degradation of QoS, ability to rapidly design, deployment and modification of QoS sensitive services. Fortunately, new emerging NC&M concepts try to eliminate these drawbacks. Some of these concepts are presented in the next section.

3.2 New Approaches to Network Control and Management

Recent developments in transmission and processing speeds as well as in distributed software engineering have the potential to create a new environment to deploy a myriad of new sophisticated services, including multimedia. However, to make it happen current close and monolithic network environment should become *open and programmable.* The term *open* means that standard *Application Procedure Interfaces* (APIs) are used to access network elements (e.g. routers, ATM switches) and basic network services. The term *programmable* refers to flexibility achieved by using high level languages to (a) represent the functionality of network resources by a set of software abstractions; and (b) access (manipulate), through APIs, the capabilities of these resources.

There are a number of activities around the world investigating these issues. Below, several better known approaches reflecting general trends are briefly presented.

3.2.1 TINA

The *Telecommunications Information Networking Architecture* (TINA) is probably one of the most widely known conceptual architectures that enable the creation of distributed multimedia services. It tries to integrate the strengths of traditional telecommunications (i..e. high security, reliability, QoS) with the power of users' computers and software capabilities. TINA aims at provisioning any kind of multimedia service, running on a global scale, on different network technologies (e.g. IN, ATM, Internet) and any type of connectivity, including multiparty connections.

The *TINA Consortium* (TINA-C) is composed of representatives of almost all major telecommunications players. After a slow start in 1990, it completed in 1997 work on an architectural framework, component specifications, and demonstration of feasibility [INOU98]. In 1998, it started the second phase of the commercial adoption of its architecture. By the year 2000, a large-scale deployment of TINA-conforming products and TINA-based services is expected [TINA97].

The TINA-C main objectives are:

- *Separation of the connectivity software from the switching hardware* – this separation is obtained by using open connection management interfaces and specifying both service and terminal connectivity reference points.

- *Integration of control (signalling) and management* - TINA aims at replacing SS7 and TMN. However, seamless service provisioning for both existing technologies, such as Intelligent Network and TMN, and new ones like ODP is assumed. Much effort is spent to create mechanisms (e.g. various gateways) to enable smooth transition from old to new technologies. For example, several different approaches have been proposed to enable a smooth TMN to TINA transition [PAVO98].

- *Adoption of distributed-objects technology* for the creation of a generic computing and communication platform – TINA follows the OSI *Reference Model of Open Distributed Processing* (RM-ODP). Various controllers, which run on general purpose distributed platforms exchange information through local and remote invocations. Although these interactions resemble signalling activities, they are expressed in terms of high level operations [LAZA97].

- *Support for QoS* - QoS requirements are declaratively specified using the computational and engineering viewpoints (see below);

- *User and service mobility support* – one of the aims is to enable the creation of multimedia services for mobile/wireless users using technologies such as GSM and UMTS.

Modelling in TINA follows several inter related viewpoints, namely [TINA98]:

- The *enterprise viewpoint* - defines business roles of the parties (e.g. network providers, service providers, users) involved in a cooperative solution being implemented in an open and deregulated market. TINA defines a set of reference points (not all fully specified yet) providing specification of interactions between separate administrative domains. Both manager/agent and peer-to-peer relationships are allowed.

- The *information viewpoint* – specifies information entities and relationships between them (e.g. composition, containment);

- The *computational viewpoint* - describes data types, interfaces and functions of computational objects. TINA *Object Definition Language* (TINA-ODL), being a superset of the *Object Management Group's* (OMG) *Interface Definition Language* (IDL), is used for computational modelling. In this viewpoint, QoS parameters required to provide guarantees to objects are specified as service attributes.

- The *engineering viewpoint* (see Fig.1) – defines distribution of objects in a network based on a *Distributed Processing Environment* (DPE), a logically separated signalling network called *kernel transport network* (kTN), and the *Network Computing and Communication Environment* (NCCE) containing operating systems, communication protocols etc. At this level, *resource managers* use various mechanisms to achieve QoS.

The *Common Object Request Broker Architecture* (CORBA), being an industry standard developed by OMG, is currently used as TINA's DPE. Assuming the use of CORBA (Version 2) and taking into account current developments in TINA, the requirements for M-NC&M listed in Section 2 can be supported as follows:

1. *Covering traditional management functions.*

   As mentioned above, TINA assumes incorporation of all TMN functions. It also assures a smooth transition from TMN-like to full TINA management.

2. *Military QoS and its graceful degradation.*

   TINA inherently supports QoS. An essential feature of the TINA architecture is that each network element (e.g. IP router, ATM switch) advertises its resources and makes them accessible to algorithms running outside the element. This feature should enable to achieve M-QoS and graceful degradation of QoS by appropriately manipulating resources in network elements.
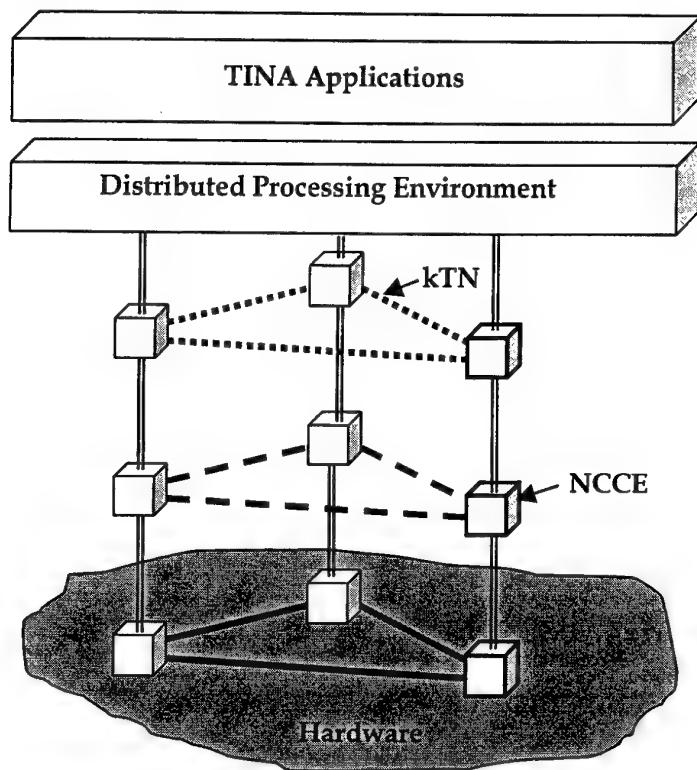

Figure 1. General TINA model.

3. *Covering heterogenous environments and networks.*

The TINA architecture targets all possible environments and networks, including the IP networks and ATM, thus enabling global connectivity.

4. *Security.*

The use of CORBA for network control allows for the utility of a very broad range of security mechanisms. The current security specification defines Application Programming Interfaces (APIs) that provide access to security services supported by a number of different, potentially replaceable security architectures and mechanisms [AIDA98]. The security services include authentication, protected message exchange, access control, security auditing. Since network management in TINA will be based on CMIP, its security aspects are as for TMN. It is noted that there is a special interest group created within TINA-C to deal with security issues.

5. *Support of multimedia/multiparty applications.*

A strong feature of the TINA architecture is its ability to handle multipoint-to-multipoint connectivity and complex communication sessions based on multimedia services.

6. *Deployment of new services.*

Using open programming architecture and DPE such as CORBA enables rapid development of new services. CORBA provides a flexible object oriented environment to build distributed services and facilitates integration of control and management.

7. *Robustness.*

The use of CORBA provides the means to build robust distributed control and management infrastructure. Note that CORBA, as CMIP, uses the connection-oriented reliable transport paradigm. It offers more flexibility for distributed control and management platform than TMN or the Internet. The basic difference lies in the ability to hide from applications the location of objects. This feature enables creating and changing reusable, portable and distributed object-oriented management software in distributed heterogenous environments.

8. *Performance.*

Using CORBA to establish a flow through a network can be performed in various ways including a parallel approach in which all network nodes are accessed at the same time, faster than when using the (hop-by-hop) SS7 approach.

Concerns have been raised about poor performance of some applications using CORBA middleware. More research is required to establish the influence of CORBA communication mechanisms and processing overheads on network management performance, particularly in an impoverished environment. It is noted that there are pending research efforts to develop real-time CORBA end-systems [SCHM97].

25

9. *Scalability.*

   CORBA provides all the facilities required for a scaleable distributed management infrastructure.

10. *Use of industry standards.*

    The use of CORBA middleware for network management in TINA creates a solid, well-standardised software platform. Note that an increasing number of (distributed) applications are being built using CORBA thus proving its applicability on one hand and thoroughly testing its features on the other. Although TINA's specification is not yet fully standardised, there are several commercial products supporting application design.

It is noted that several successful international field trials using a CORBA-based implementation of the TINA architecture have been held in 1997-1998 to demonstrate the main concepts, including handling a multidomain, multiservice, multinetwork environment [INOU98]. It seems that the final success of TINA very much depends on:

- The pace of TINA-C's standardisation efforts (particularly in relation to reference points) enabling to create a full range of tools supporting the development of applications, as well as NC&M software according to the TINA methodology;

- The complexity of TINA's structures (and the related performance) compared with other commercially available solutions.

3.2.2 XRM

The *Extended Integrated Reference Model* (XRM) [CAMP97, LAZA96, LAZA97] has been developed by the COMET group at Columbia University. It is a modelling framework for *open* control and management of broadband networks and multimedia computing platforms supporting end-to-end QoS. The XRM distinguishes three layers with APIs between them, namely (see Fig. 2):

- *The Broadband Network.*

  This layer is composed of physical resources such as network equipment (ATM switches, IP routers/switches etc.) and multimedia end-devices, as well as logical resources (e.g VPIs, VCIs). The layer offers to the upper layer, the Multimedia Network, a set of APIs that abstract states of these resources and represent QoS abstractions derived from the media-unaware broadband network. These interfaces enable remote monitoring, control and management of the resources.
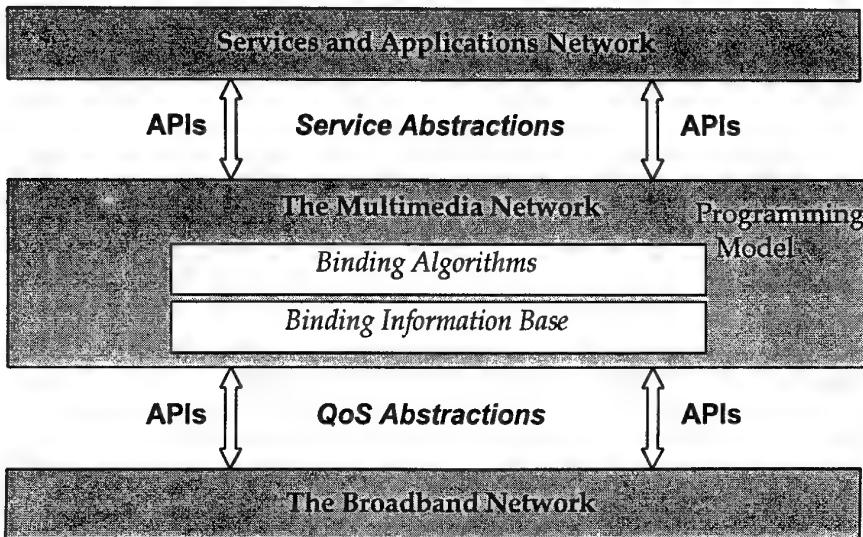
Figure 2. General decomposition of the XRM model

- *The Multimedia Network.*

  The main function of the layer is to provide the middleware to facilitate creating multimedia service abstractions in the form of APIs representing basic services with end-to-end QoS guarantees. These abstractions are stored in the *Binding Information Base* (BIB) which is a distributed repository of information encapsulating the state of the broadband network. APIs in the BIB are seen as building blocks of network services. In addition, *binding algorithms* used in the process of creating these services are specified at this layer.

- *The Services and Applications Network.*

  Network services and applications are created at this layer assembling basic services stored in the BIB and selected binding algorithms of the lower layer.

Two important concepts have been developed for the Broadband Network layer:

- *Schedulable region,* to characterise the transmission capacity of ATM switches.

  Switching bandwidth and link capacity in a switch are specified as a function of a limited number of traffic classes used for circuit emulation, voice and video, data and network management. Each of these classes is characterised by different statistical properties (e.g. cell loss, delay) and QoS requirements [HYMA93]. A region (hyperplane) is built for each output buffer in a switch to specify the

maximum number of calls of each type that could be accepted while still guaranteeing expected QoS for all calls.

- *Multimedia capacity region*, to specify the capacity of end-system devices.

  Multimedia end-devices (e.g. video cameras, microphones) are perceived in XRM as systems having their own QoS constraints, such as frame delay or loss rate. Several classes of services (e.g. MPEG-I, MPEG-II, CD-audio) are distinguished for these devices, and a capacity region specifies the maximum number of calls which can be admitted that still do not overload the end-device.

When a call is to be established, the control system only admits the call if there are enough resources in all switches/end-devices along the path, so that QoS of already established calls is not deteriorated. This corresponds to keeping the point of operation below each involved schedulable region/capacity region.

Since 1994, the XRM architecture has been implemented by the COMET Group in their experimental ATM, CORBA based and programmable platform called XBIND. This platform has been recently extended to include a software middleware platform called *Mobiware* to support QoS controlled mobility in future wireless media systems [CAMP96].

Although the XRM architecture is general and potentially covers all NC&M activities in a multimedia network, only those related to service control and management have been analysed in detail and tested, particularly using the XBIND platform. The XBIND experimental software (including Mobiware) is available from COMET Group. It is noted that Communication Division at DSTO is testing currently the applicability of this software for military applications.

3.2.3 IEEE P1520 Standards Initiative

In 1997, several companies (e.g. Ericsson, DEC) and laboratories initiated a new IEEE standards initiative, called *P1520*, to define a reference model for programmable network interfaces [P1520]. This model distinguishes several levels (see Fig.3) composed of entities and separated by programmable interfaces specified in terms of industry standard *Interface Definition Language* (IDL). The levels correspond to end-user applications, value-added services, network generic services, virtual network devices, and network physical elements. Each interface is an API open for distributed access. From the viewpoint of this report, there are two important advantages of this model, namely (a) open access to network elements (e.g. switches and routers) by services; and (b) separation of control and management applications from network elements.
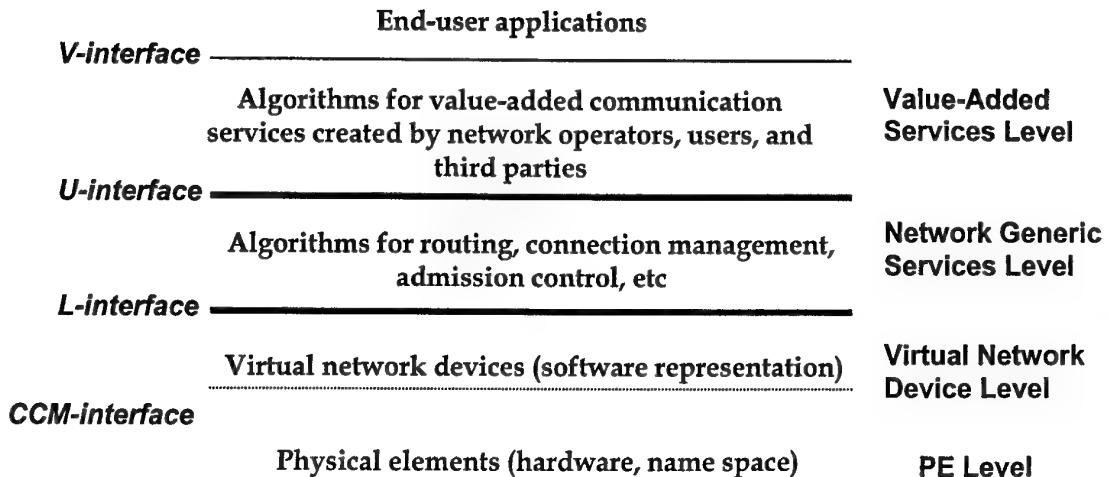
End-user applications

V-interface ────────────────────────────────

Algorithms for value-added communication
services created by network operators, users, and
third parties

U-interface ════════════════════════════════

Algorithms for routing, connection management,
admission control, etc

L-interface ════════════════════════════════

Virtual network devices (software representation)

CCM-interface

Physical elements (hardware, name space)

**Value-Added
Services Level**

**Network Generic
Services Level**

**Virtual Network
Device Level**

PE Level

Figure 3. The P1520 reference model

The levels of the model are:

- *Value-Added Services Level* (VASL) - entities at this level are end-to-end algorithms that add value to services provided by lower levels. These algorithms include real-time stream management, synchronisation of multimedia streams etc;

- *Network Generic Services Level* (NGSL) – this level offers (network-wide) generic services to VASL including routing, configuration and admission control. These services are delivered using (distributed) algorithms stored at this level;

- *Virtual Network Device Level* (VNDL) - this level contains entities (objects) that are logical representations (abstractions) of physical elements at the lowest, physical level;

- *Physical Elements* (PE) *Level* – all physical elements of the network reside at this level. These elements are accessed using open protocols. Note, that the interface between this level and VNDL is not a programming interface but rather a collection of protocols (e.g. GSMP, CMIP, SNMP).

The P1520 document also suggests the mapping of the proposed interfaces to various types of networks, including ATM, IP (both using routing and switching), SS7 and TINA. By the end of year 1999, the group plans to deliver for ATM switches full specification and software for interfaces L and CCM. It will also examine interfaces U and L for IP routers and switches.

3.2.4 Summary

The new NC&M concepts presented in this section clearly address the problem of rapid design, deployment and modification of sophisticated (multimedia) services. Additionally, these concepts support separation of network control and management from physical switching infrastructure thus enabling to use generic network control and management software for various transportation mechanisms (e.g. ATM, IP) and environments (e.g. fixed, mobile).

A common feature for TINA, XBIND and P1520 that is crucial to delivering M-QoS, is that each switch/router advertises its resources making them accessible to controllers. These controllers run algorithms on a general purpose *Distributed Processing Environment* (DPE) platform such as CORBA. The above feature enables control activities to be expressed in terms of high level operations instead of (traditional) low level mechanisms, thus creating high flexibility in manipulating switch/router resources. Basic concepts of these architectures have already been validated by numerous demonstrations using experimental software (e.g. see [OLIV98, INOU98, CAMB97, MING98]). In our opinion, these concepts have a good chance to be accepted by the commercial world. To check the applicability of these concepts to deliver M-QoS, we have created an architectural framework for M-NC&M and implemented it as a demonstrator in an ATM environment. The next section presents basic features of this framework. The ATM demonstrator is described in Section 5.

4. The Proposed Architectural Framework

4.1 Basic Features

To fulfil the requirements described in Section 2, it is proposed that the M-NC&M architecture be characterised by the following fundamental features:

1. Two basic classes of traffic will be distinguished by M-NC&M:

    a) *Military essential traffic* (M-traffic) - this traffic type will be supported by M-QoS mechanisms (see next section), including prioritisation and preemption of flows depending on their military value.

    b) *Non-military essential traffic* (NM-traffic) – only the "best effort" service, in case of IP networks, and the lowest possible priority in ATM networks is offered to information flows.

2. *Distributed Programming Environment (DPE)* paradigm will be broadly used by M-NC&M, particularly for service control and management;

3. *M-NC&M will conform to an open and programmable environment.*

The general open programming model for creating services in ADF integrated networks, is presented in Fig. 4. This model utilises concepts common for TINA, XRM and P1520. We have not decided yet which architecture(s) in particular should be used as a basis for the M-NC&M since the potential candidates are not yet fully developed and standardized. The following basic levels are distinguished:

*   *Physical Network (PE) Level.*

    It includes physical devices, such as switches, routers and end-user devices used to build the ADF communication infrastructure covering fixed, mobile and satellite environments. As pointed out in Section 2, different environments (i.e. fixed, mobile, satellite) with specific features (e.g. transmission latency) and transportation technologies (e.g. IP, ATM, IP-over-ATM) can be used. Hence, appropriate components are depicted in Fig. 4. This level offers to the next level access to physical devices using various protocols, such as CMIP, SNMP or GSMP.

    In TINA, the functions of this level are covered by both the *Network Computing and Communication Environment* (NCCE). In XRM this level is called *Broadband Network.* Finally, in draft standard P1520, the functions of this level correspond to those of the *Physical Element* (PE) level.
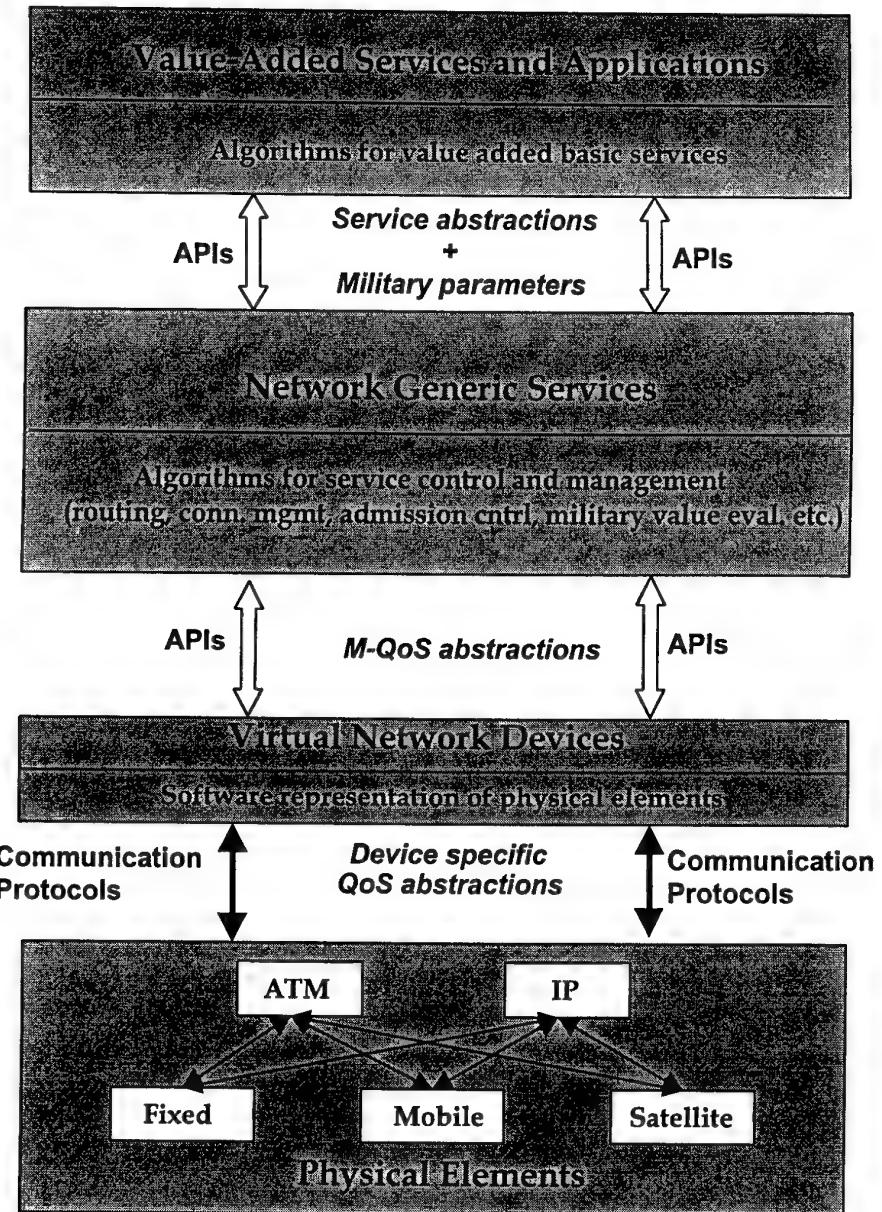
Figure 4. Model of open and programmable environment for multimedia military networks.

- *Virtual Network Devices Level* (VNDL).

  APIs offered to the upper level are distributed software entities that abstract both physical devices and their states. In other words, real devices are seen through these APIs as virtual devices. M-QoS requirements are specified through the APIs and they are translated through the interface with the PE level to:

  - Device specific QoS parameters (e.g. CBR with a particular peak rate ate an ATM switch) exchanged with the PE level;
  - Values of parameters used for device mechanisms involved in manipulating flows (e.g. values of parameters for a leaky bucket mechanism used to shape less important flows).

  In TINA, the functions of this level are covered by both the *Network Computing and Communication Environment* (NCCE) and *kernel Transport Network* (kTN). In XRM this level is called *Biding Interface Base (BIB)*. Finally, in draft standard P1520, the functions of this level correspond to those of the *Virtual Network Devices Level* (VNDL).

- *Network Generic Services Level (NGSL)*.

  This level is responsible for proper functioning of the network. It includes all algorithms for network control and management including those responsible for: (a) evaluating values for military parameters characterising information flows; (b) invoking functions to manipulate information flows (e.g. shaping less important military flows). In addition, these algorithms are used to accomplish end-to-end QoS guarantees. This level offers to the upper level the APIs through which *generic services* with guaranteed characteristics and required values for military parameters can be invoked. An example of such service is a point-to-point CD audio connection with given peak cell rate, cell loss rate, maximum number of lost cells in a gap, bound on the transmission delay, mission priority and time relevance.

  TINA's *Distributed Processing Environment* (DPE) is an equivalent of this level. In XRM, *The Broadband Network* covers the same functions. In case of the draft standard P1520, the *Network Generic Services Level* (NGSL) performs the same functions.

- *Value-Added Services and Applications (VASAL)*.

  In this level, generic services from the NGSL can be bundled to create *a value-added service* with user oriented features, such as synchronisation of multimedia flows. Specific user applications can be built and deployed within this level using both generic and value-added services.

  As for the TINA (engineering) model, the *TINA Applications* component is the counterpart to this level. In the XRM model, the *Services and Applications Network* component perform equivalent functions. As far as the draft standard P1520 is

concerned, the same set of functions is covered by the *End User Applications* component and *Value-Added Services Level* (VASL).

It is noted that all functions of VNDL, NGSL and VASAL are implemented in a *Distributed Processing Environment* (DPE) middleware such as CORBA. It also should be noted that the above model enables to specify Network Control and Management functions at the NGSL and VASAL transparently to the underlying transmission technology specified at the PE level. This will enable to overcome (to a major extent) the uncertainty expressed in Section 2 in relation to the future developments in the transportation technologies.

The presented above model for creating and deploying services should be accompanied by model(s) for performing all traditional management functions described in Section 2. There are several possible approaches to creating such models. For example, the same model as presented for service control and management can be applied enabling to achieve reusability of the same objects and economy of scale. However, other factors may also play an important role, such as the amount of legacy management software, security and robustness of the used DPE (e.g. CORBA) versus those offered by TMN (CMIP) etc. More detailed investigation is required to compare such models when applied to the ADF networks.

In the next section, we will analyse in more detail specific mechanisms supporting M-QoS in the presented service model.

4.2 Support of Military QoS

In order to achieve end-to-end M-QoS, a set of mechanisms should be implemented both in the network and in Customer Premises Equipment (CPE). Following a classification presented in [AURR98], these mechanisms can be categorised as follows[2]:

- *M-QoS Provision Mechanisms;*
- *M-QoS Control Mechanisms;*
- *M-QoS Management Mechanisms.*

The following sections present these mechanisms in more detail.

---

[2] Classification given in [AURR98] refers to commercial networks. In this report, it is used in relation to military networks.

4.2.1 M-QoS Provision Mechanisms

M-QoS provision is responsible for flow establishment with end-to-end M-QoS guarantees. It comprises the following mechanisms:

- *M-QoS mapping*

  This mechanism is used to automatically translate M-QoS requirements specified at a higher level of the model to the requirements for the lower level. For instance, end-to-end QoS of a video flow expressed at VASAL (cf. Fig. 4) in terms of frames has to be translated by an algorithm at NGSL to a cell/packet specification at the PE level for each traversed link. An interesting framework for end-to-end QoS mapping between various levels of the transport protocol stack is presented in [HUAR97].

  The military value specification given at VASAL has to be analysed by an appropriate algorithm(s) at NGSL to obtain for each related flow its priority value. Note that depending on the policy used, this value can change during the flow, for example because of the specified time relevance parameter. A separate study is required to find appropriate formula(e) calculating the military value of a flow as a function of factors listed in Section 2.

- *Admission testing.*

  The aim of this mechanism is to find out whether the required M-QoS can be fulfilled by the network. The answer depends on the network resources management policy and availability of resources. If there is not enough of them, prioritisation/pre-emption will be used to establish flows that are more important.

  Fig. 5 shows a flow chart representing the proposed general admission policy for a new flow to be established. If there are enough resources in each node along the path, then the request for the flow should be accepted. Otherwise, it should be calculated whether sufficient amount of resources could be obtained by throttling existing flows of lower military value. If this is the case, the request should be accepted. If not enough resources can be obtained by throttling, the request should be rejected. After rejection the user may:

  - Request a lower M-QoS for the flow;
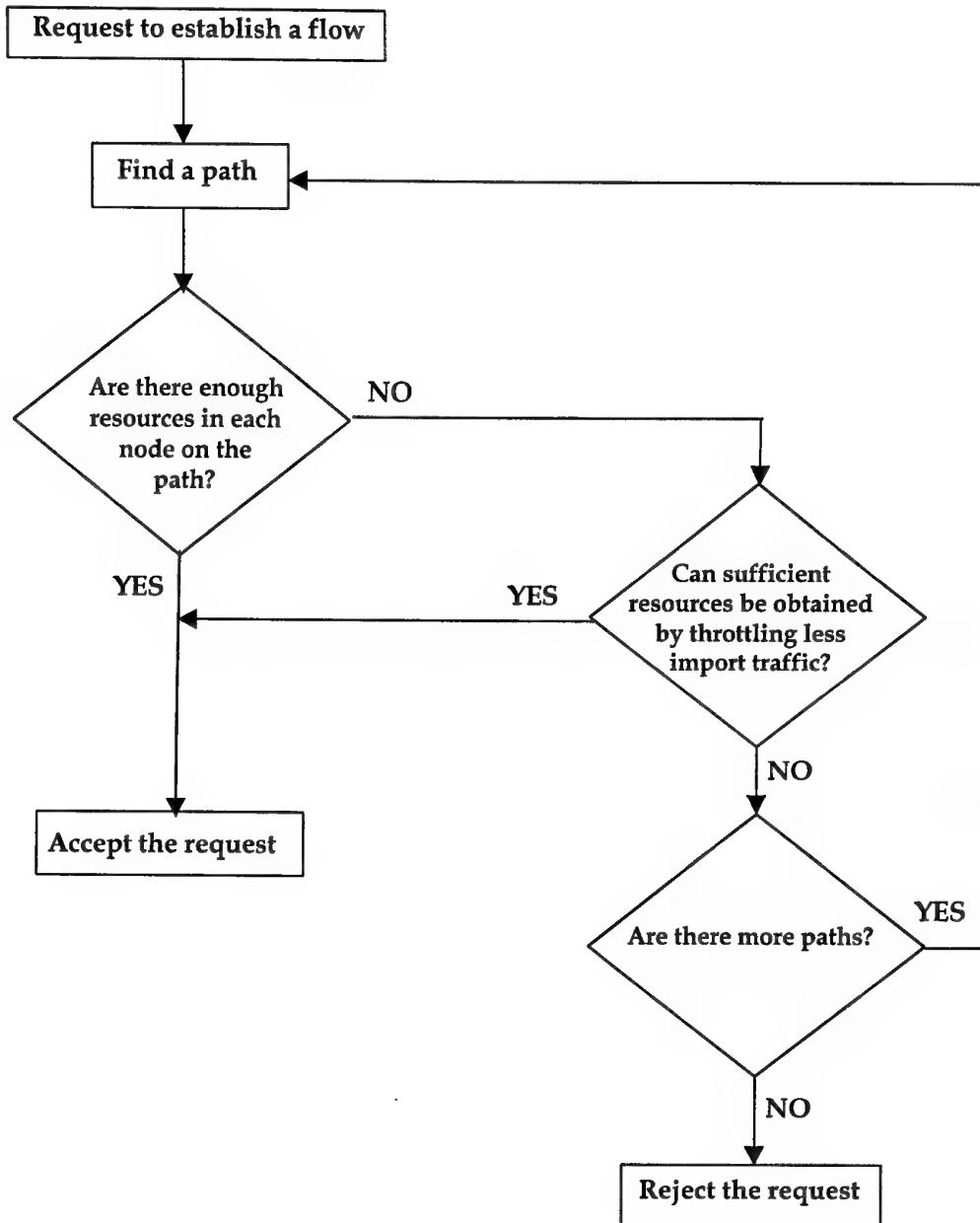 - Use best-effort service (always accepted);
  - Quit.

Figure 5. *The proposed admission testing policy.*

In the proposed policy, it is assumed that:

- Whenever a flow of a higher military value is admitted at the cost of other existing flow(s), the latter one(s) are appropriately shaped by a flow shaping mechanism (see below);

- The positive result of admission testing in a node causes only reservation of a resource. Only when admission tests in all involved nodes are positive, commitment of the reserved resources is applied and, if required, flow shaping of other flow(s) is implemented.

Admission testing in nodes can be done:

- *Sequentially*, where a connection controller queries all nodes hop by hop along the path; or

- *In parallel*, where the connection controller queries all involved nodes at the same time.

More research is required to compare performance aspects of both approaches in different military environments (i.e. fixed, mobile and satellite).

- *Resource reservation protocols.*

  These protocols are responsible for end-to-end allocation of the resources in a network (e.g. in switches, routers) and end-systems (e.g. CPU, memory, I/O devices) for a flow, according to the M-QoS specification. Such allocating starts once a path for the flow is found. Standard commercial protocols (e.g. RSVP) are assumed to use by M-NC&M.

4.2.2 M-QoS Control Mechanisms

These mechanisms are used to perform real-time traffic control to support M-QoS of admitted information flows. The mechanisms include:

- *Flow shaping.*

  This mechanism is used to shape flows as they traverse the network according to the traffic descriptors delivered by the end-user during flow admission. Examples of such descriptors include peak rate, sustainable rate, and burst tolerance.

  In military networks, shaping of flows of lower military value can be required due to:

  - Admission of a flow of a higher military value;

- Unexpected deterioration of available resources (e.g. lowering of satellite link capacity due to errors) and the resulting necessity to maintain QoS of a flow(s) of higher military value.

In both cases, it is proposed to start the shaping from the lowest priority level and proceed upwards. Using this approach, the problem of shaping distribution among flows of the same priority level must be resolved. *Should it be imposed on each of them, or rather on a few (and the rest be left intact)?* Although the former approach is harder to implement and involves more processing/control messages, deterioration of QoS is more evenly distributed among the flows. This problem needs further study.

Distribution of (control) information among network nodes and end-systems about newly imposed shaping is another problem that requires more research. For instance, when a flow is to be shaped at a given node, it might be beneficial to pass information about this shaping to all nodes traversed by the flow and the source end-system. As a result of this action:

- The traversed nodes can shape the flow as well, and thus released resources could be used for other flows.

- The source end-system can immediately impose any M-QoS adaptation mechanisms (see M-QoS Management Mechanisms below). If these mechanisms cannot cope with the deterioration of transmission, source and destination users can be notified that the network cannot maintain the promised QoS.

The above approach may impose, however, heavy control traffic affecting scalability and may prevent regaining of resources by impoverished flows once the reason for shaping disappears.

Finally, a problem of distributing newly acquired bandwidth (e.g. due to the release of bandwidth by a flow or because of improvement of transmission conditions) among throttled flows should be analysed.

- *Flow scheduling*

This mechanism is responsible for scheduling of media units (e.g. video frames) in end-systems, and packets/cells in network nodes. Some examples of different scheduling disciplines can be found in [KURO93]. Scheduling mechanisms used in commercial networks should suffice to fulfil the requirements of military networks.

- *Flow policing*

This is used to check whether the statistical properties of an information flow produced by the end-user adhere to those specified when admitting the flow. If this is not the case, the flow shaping mechanism is used to regulate the flow. Flow policing is very important in military networks to protect against misbehaving

users. It should be implemented at all interconnection points where the network cannot trust the conformance of the sent traffic, particularly:

- Between the military network and a commercial carrier;
- Between an end-system and the military network.

Standard mechanisms, such as *Leaky Bucket* or *Generic Cell Rate Algorithm* [ATMF96] can be used for flow policing by M-NC&M.

- *Flow control*

  This is used to adjust the rate a source sends information to a network. Two types of flow control can be used for this purpose:

  - *Open loop flow control,* where the source sends information according to the contract with the network established during flow admission;
  - *Closed loop flow control,* where the rate from the source is adjusted to feedback received from the destination.

  An example of the use of the latter approach in an ATM environment is proposed in [HUAR96], where the authors use a separate connection to pass feedback from the destination to the source. It is expected that the same flow control mechanisms as in commercial networks will be used by M-NC&M.

- *Flow synchronisation*

  These mechanisms are related to event ordering and timings of multimedia interactions, such as audio and video synchronisation flows at the receiving end-system. Special flow synchronisation protocols are used for this purpose. Compared with commercial applications, military ones do not seem to impose any additional requirements for these mechanisms.

4.2.3 M-QoS Management Mechanisms

These mechanisms operate on a slower time scale than M-QoS control mechanisms. They are used to ensure that the QoS promised by the network is sustained. The following management mechanisms can be distinguished:

- *M-QoS monitoring.*

  This mechanism is used to collect statistics (typically delays and loses) for each transportation level (e.g. frame level, packet level) involved in delivering QoS. Different time scales are used for this purpose at different levels. Monitoring can be done either end-to-end (as a part of transport level feedback mechanism) or locally by an end-system (e.g. to support packet scheduling) [AURR98]. Military aspects of

QoS do not imply additional requirements for this mechanism. As pointed out in [HUAR96], the definition of a good measurement time interval during which monitoring is performed is an important and hard to solve issue. This problem needs investigation.

- *M-QoS maintenance.*

  This mechanism is used to compare results of monitoring the ongoing QoS (see above) with the contracted QoS. In case of disproportion between them, additional tuning mechanisms must be invoked (e.g. applying a different flow regulation scheme to improve throughput). The same mechanism(s) as for commercial networks are expected to be used by M-NC&M.

- *M-QoS degradation.*

  This mechanism is applied to indicate to the end-user that its QoS cannot be maintained using M-QoS maintenance mechanisms. Such a situation can be caused by deterioration of transmission capabilities or admission of a flow of a higher military value. Upon the indication, the end-user can:

  - Take no action
  - Invoke an M-QoS scalability mechanism(s) (see below) to adjust to new conditions. Note that this may be done automatically;
  - Re-negotiate with M-NC&M a lower M-QoS;
  - Quit the service.

  It is expected that the same mechanisms as used in commercial networks for QoS degradation will be used by M-NC&M.

- *M-QoS availability.*

  It enables the application to define intervals during which the network monitors various QoS parameters (e.g. delay, loss). When an interval finishes the application is informed (by receiving a signal) about the value of a given QoS parameter during this interval. Commercial QoS availability mechanisms are expected to be used by M-NC&M.

- *M-QoS scalability.*

  It is expected that the same mechanisms as for commercial QoS scalability will be used by M-NC&M. These mechanisms can be divided into the following two groups:

  - *M-QoS filtering,* which is applied to scale flows as they traverse the network. An example of such mechanisms is translating one encoding mechanism to another. This type of scalability is particularly useful when multicasting

communication is performed with different end-system QoS capabilities [YEAD94];

- *M-QoS adaptation,* which is used at the edge of the network to monitor and adjust of flows to QoS fluctuations offered by the network. Such mechanisms include discarding less important information in case of MPEG-II, using different sampling mechanisms for audio service etc.

5. Case Study: ATM environment

In 1998, the principles of the framework proposed in the previous section have been successfully applied by Communication Division, DSTO, in a demonstrator that manages and offers basic multimedia services with M-QoS. The demonstrator is implemented on an ATM broadband communications infrastructure called EXC³ITE. This infrastructure offers a distributed object-oriented environment intended to aid the development of future Australian Defence C⁴I capabilities through the integration of new and prototype architectures.

5.1 Physical Infrastructure

Fig. 6 shows the basic communications infrastructure of the demonstrator. It has been designed to test some aspects of multimedia service management over a resource impoverished satellite link connecting a deployed node to a core network. In this infrastructure, a number of ATM multimedia end-stations are connected via ATM switches from two different manufacturers.
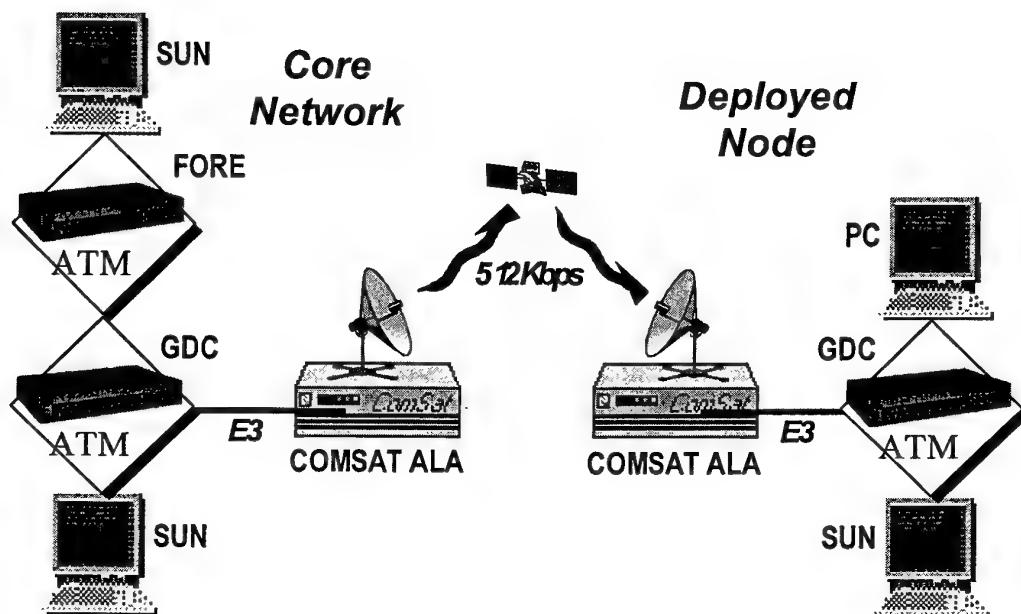

Figure 6. Experimental ATM infrastructure.

The demonstrator also includes ATM Link Accelerator (ALA) devices supporting the use of the satellite link. These devices are responsible for monitoring bit error rates over the link and selecting appropriate levels of Reed-Solomon coding in order to maintain acceptable cell loss ratios. The error rate fluctuations result in changes to the available link capacity, which are reported from ALAs to the M-NC&M system.

5.1 Implementation of M-NC&M Framework

The experimental M-NC&M architecture is shown in Fig. 7. To create the NGSL and VNDL levels we used XBIND software, which has been modified and value-added to address the M-QoS requirements described in Section 4. The CORBA middleware technology provides the building platform to solve problems of equipment heterogeneity and distribution of objects representing network resources (e.g. physical devices, their states and various algorithms). CORBA also offers the required flexibility in applying alternative algorithms to deliver M-QoS through high level programmability.

The meaning of objects depicted in Fig. 7 is as follows:

- *VirtualSwitch* is an interface providing a consistent standard view of an ATM switch fabric, encapsulating the state of the target device. Methods operating on this object provide the capability to manipulate virtual connections and their M-QoS characteristics.

- *VirtualLink* is an interface providing a consistent standard view of an ATM switch output port and associated link characteristic, encapsulating the state of the target elements. Methods operating on this object assure the capability to manipulate output buffer resource allocations stored as *ResourceShaper* objects.

- *VirtualDevice* is an interface providing a consistent standard view of a specific end-device capability, offering services to the architecture. Methods operating on this object allow for manipulating of the device capability characteristics stored as *EndResource* objects.

- *Connection Manager* is an algorithm operating upon a number of virtual objects, with the role of providing a connection service within its designed domain of control. This service includes mapping of user QoS requirements to transport level requirements, reservation of resources, route selection, and reservation of switching table entries.
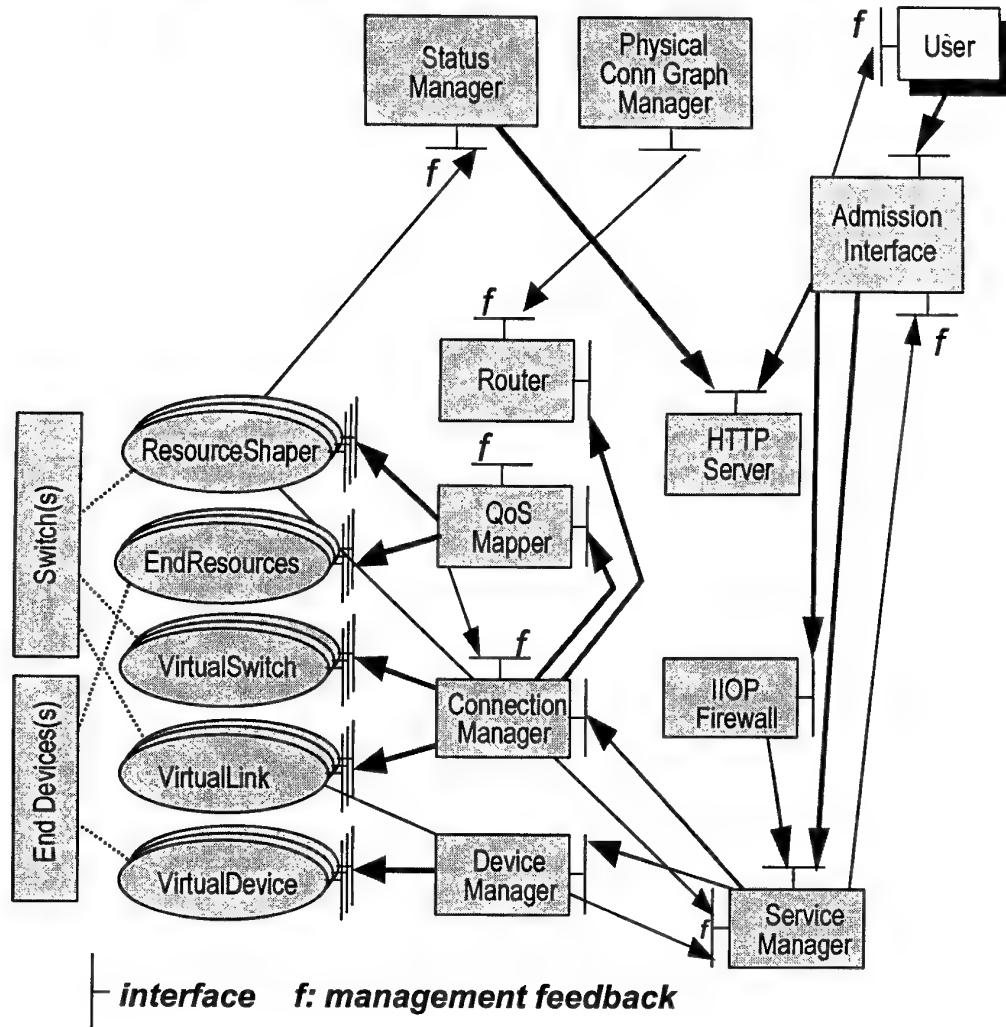
43

Figure 7. Experimental M-NC&M architecture.

- *Device Manager* is an algorithm operating upon a number of VirtualDevice objects, with the role of managing end-device capabilities. This service includes mapping of user level M-QoS requirements to application level requirements, compatibility assurance, capability lifecycle management and customisation.

- *Route Manager* is an algorithm providing specific route profiles through the network topology, within its designed domain of control.

- *Physical Connection Graph Manager* is an algorithm maintaining a view of the current network topology, within its domain of control. Currently this is only static.

- *Service Manager* is an algorithm providing an abstract interface to user applications for the role of creating service instances, within its designed domain of control. This service includes authorisation and a managed delegation role to facilitate simplex service creation.

- *Status Manager* is an algorithm enabling an abstract interface to user applications to solicit current network and service status, within its domain of control. This service includes gathering of discrete event information and fusing of collected data.

The NGSL offers to applications residing at the VASAL level a number of generic ATM services, including point-to-point connections for voice, video and file transfer. Each such service has associated military parameters. Currently, only the mission priority parameter is considered. To fulfil generic services, the NGSL comprises a collection of objects providing distributed algorithms for basic service control and management functions, such as routing, admission control, connection establishment and management, as well as M-QoS provision (e.g. calculating military values, QoS mapping between M-NC&M levels).

The VNDL encapsulates the state of the ATM switches and end-station devices. Near real-time control of these devices at the PE Level is achieved using cached SNMP manipulation of device Management Information Bases (MIBs).

As stated in Section 4, fine shaping of flows with lower military value is required to achieve graceful degradation of QoS in overloaded military networks. To accomplish this, the experimental M-NC&M invokes in ATM switches the *Generic Cell Rate Algorithms* (GCRAs) [ATMF96] under direct MIB manipulation. Note that the GCRA is supported for all service classes (e.g. CBR, VBR) and all input connections in a standard ATM switch. A simple algorithm has been prepared to shape CBR connections of lower military values at a switch in order to acquire free link capacity for a more important (CBR) flow. The design of a similar algorithm(s) to shape a mixture of CBR, VBR and ABR traffic flows is under study.

The current experimental M-NC&M implements service management in a centralised manner, that is, the algorithms (e.g. Connection Manager, Service Manager) in NGSL and VASAL are centralised. A distribution of these algorithms can improve service survivability (avoidance of single points of failure), scalability, flexibility and performance, particularly when services are delivered across interconnected networks. Service management architectures enabling such a distribution need further study.

In parallel to the above efforts should go the incorporation of the M-QoS awareness to user applications under construction at DSTO. To achieve this purpose, a standardised software interface between user applications and network management (i.e. between

the VASAL and the NGSL in Fig. 7) should be specified. Once this interface is available, a DSTO application will be able to specify its M-QoS requirements to a network, as well as enable the network to inform the application about any problems in delivering the promised level of service.

6. Conclusions and Recommendations

This report has argued that there is a need for creating a seamless strategic-tactical Military Network Control and Management (M-NC&M) infrastructure covering ADF heterogeneous packet/cell based environments and networks. The main aim of the report was to propose a general framework for the M-NC&M architecture covering both the strategic domain and its extensions to the tactical domain. To achieve this aim a list of requirements for the M-NC&M architecture have been specified. Among those requirements, the following essentials are not covered by the existing packet/cell based ADF networks:

- *Military QoS* - In military networks, when not enough capacity is available to send all information "at the right time" (e.g. due to congestion in impoverished links, partially destroyed networking infrastructure), messages carrying vital (from the military viewpoint) information should be delivered first. Considering military value provides greater resilience of mission-critical flows during overloads;

- *Graceful degradation of QoS* - There are strong arguments to gradually "step down" in QoS of less important military flows in overloaded networks, instead of releasing these flows;

- *Ease of deployment of new services* - The M-NC&M architecture should enable rapid design, deployment and modification of (QoS sensitive) multimedia, multiparty services.

It has been argued in the report that traditional Network Control and Management systems such as SS7, TMN and the ones used in the Internet are not capable of fulfilling the above requirements. The report has argued that a way to achieve these requirements is to create an open and programmable environment using standardised Application Procedure Interfaces (APIs). There are currently a number of activities around the world such as TINA, XRM and IEEE P1520 standard initiatives, briefly presented in this report, investigating such environments. Although concepts supported by these activities are not yet fully developed and reflected in commercially available products, they show strong technological tendencies.

The M-NC&M architectural framework proposed in this report refers to medium term (5-10 years) design goals and follows concepts developed by TINA, XRM and IEEE P1520 standard initiatives, and adds to them military specifics expected for ADF networks. A particular emphasis of the framework is put on the way the M-QoS should be supported by the M-NC&M

The report has identified a number of problems that need further study, namely:

a) The main interest is to find how particular requirements listed in Section 2 should be fulfilled within the proposed M-NC&M framework;

b) A viable scenario(s) of the evolution of management platforms currently used by Defence towards achieving the goal management architecture;

c) Separate study is required to find appropriate formula(e) calculating the military value of a flow as a function of factors listed in Section 2;

d) The problem of shaping distribution among flows of the same priority level must be resolved. It is not clear whether the shaping should be imposed on each of them, or rather on a few and the rest be left intact;

e) The performance of CORBA middleware should be analysed when applied to perform control and management functions;

f) A study is required to compare performance of sequential and parallel admission control in different military environments (i.e. fixed, mobile and satellite);

g) Distribution of control information among network nodes about newly imposed shaping requires more research. In particular, the question of whether it is beneficial to pass information about the shaping to all up-stream nodes traversed by the shaped flow should be resolved;

h) A distribution of service management algorithms should be analysed, particularly for user applications implemented across multiple ADF networks;

i) A standardised software interface between user applications under construction by DSTO and the experimental M-NC&M implemented on the EXC³ITE network should be specified.

To efficiently solve the above problems, the report recommends that DSTO should:

A. Improve liaison with Defence Information Systems Group (DISG), especially the Network Operations Centre and the Network Technical Services at Deakin, ACT;

B. Establish close collaboration with Drs Miro Kraetzl and Peter Shoubridge, Communications Division, DSTO, to utilise their expertise in network performance and survivability;

C. Launch a series of detailed studies to resolve the problems identified in this report.

In order to increase DSTO's expertise in the area of Network Control and Management, the report also recommends that DSTO should:

D. Intensify experiments on the use of available commercial and experimental software to gain practical experience in building various M-NC&M mechanisms;

E. Monitor developments in research on open and programmable networks, particularly in TINA, XRM and IEEE P1520 standard initiatives;

F. Establish liaisons with the COMET group at Columbia University since it is one of the most the most active groups conducting advanced research on open and programmable networks;

G. Establish liaisons with the US Air Force Laboratory at Rome, NY, to exchange information about M-NC&M architecture(s) currently used and planned to be implemented in US Defence networks. The Rome Laboratory is the leading US Defence research unit working on military network management issues.

Acknowledgments

References

[ACHA98]   A. Archarya, J. Li, F. Ansari, D. Raychaudhuri, "Mobility Support for IP over wireless ATM", IEEE Communications Magazine, April 1998.

[AIDA98]   "Telecommunications Network Management – Technologies and Implementations", S. Aidarous, T. Plevyak (Editors), IEEE Press, New York, 1998.

[AKIL97]   I.Akyildiz, S. Jeong, "Satellite ATM Networks: A Survey", IEEE Communications Magazine, July 1997.

[ATMF96]   "Traffic management Specification – Version 4.0", The ATM Forum Technical Committee, April 1996.

[AURR98]   C. Aurrecoechea, A. Cambell, L. Hauw, "A Survey of QoS Architectures", ACM/Multimedia Systems Journal, Vol. 6, No. 3, 1998.

[BLAC98]   P. Blackmore, "Information Scheduling in a Military Global Broadcast System", DSTO, Australia, unpublished work, August 1998.

[BLAU98]   J. Blau, "Sprint throws in its lot with ATM", Communications Week International, 29 June 1998.

[BOWM98]   L. Bowman, R. Riehl, S. Shad, "Defence Information System Network (DISN) Asynchronous Transfer Mode (ATM) Goal Architecture and Transition Strategy", MILCOM'98, Boston, USA, 1998.

[CAMP96]   A. Campbell, A. Lazar, "Xbind Extensions for QoS Controlled Mobility", Proceedings of the 2nd International Work shop on Multimedia Information Systems, West Point, NY, September 26-28, 1996.

[CAMP97]   A. Campbell, A. Lazar, H. Schultzrinne, R. Stadler, "Building Open Programmable Multimedia Networks", IEEE Multimedia, March 1997.

[CIMI98]   L. Cimini, J. Chuang, N. Sollenberger, "Advanced Cellular Internet Service (ACIS)", IEEE Magazine, Oct. 1998.

[DIBE98]   R. Dibella, "ADF's Strategic Communications Infrastructure", presentation at School of Signals, Melbourne, Australia, Nov. 1998.

[DITT96]   A. Dittrich, M. Hoft, "Integration of a TMN-based Management Platform into a CORBA-based Environment", IEEE Network Operations and Management Symposium, Kyoto, Japan, 1996.

[DU98]   Y. Du, Ch. Hermann, K. May, S. Hulyarkar, D. Evans, "Wireless ATM LAN with or without Infrastructure", IEEE Communications Magazine, April 1998.

[ELMO98]   F. EL-Mokadem, "Evaluation of Network Performance Objectives over DISN ATM Connections", MILCOM'98, USA, 1998.

[FLAH98]   M. Flaherty, "Strategic Planning Workshop for Military Information Networks Branch", DSTO internal document, Nov. 1998.

[FERG97]   P. Ferguson, "Simple Differential Services: IP TOS and Precedence", Internet Draft, Nov. 1997.

[GRAF98]   Ch. Graff, M. Bereschinsky, M. Patel, "Application of Mobile IP to Tactical Mobile Internetworking", MILCOM'98, Boston, USA, 1998.

[HADJ98]   S. Hadjipanteli, P. Kumar, S. Wang, "Defense Information system Network (DISN)/NIPRINET Modelling and Analysis for Unclassified ATM Network", MILCOM'98, USA, 1998.

[HUAR96]   J.F. Huard, I. Inue, A.A. Lazar, H. Yamanaka, "Meeting QoS Guarantees by end-to-End QoS Monitoring and Adaptation", Workshop on Multimedia and Collaborative environments of the 5th IEEE International Symposium on High Performance Distributed Computing, Syracuse, USA, 1996.

[HUAR97]   J. Huard, A. Lazar, "On End-to-End QoS Mapping", Proceedings of the 5th IFIP Workshop on Quality of Service, New York, USA, May 1997

[HYMA93]   J.M. Hyman, A. Lazar, G. Pacifici, "A Separation Principle Between Scheduling and Admission Control for Broadband Switching", IEEE Journal on Selected Areas in Communications, Vol. 11, No. 4, May 1993.

[INOU98]   Y. Inoue, D. Guha, H. Berndt, "The TINA Consortium", IEEE Communications Magazine, Sept. 1998.

[INTS94]   R. Braden, D. Clark, S. Shenker, "Integrated Services in the Internet Architecture: an Overview", Internet RFC 1633, June 1994.

[JOHA96]   K. Johannessen, "Security of TMN", IEEE Network Operations and Management Symposium, Kyoto, Japan, 1996

[KONG96]   Q. Kong, G. Chen, "Integrating CORBA and TMN Environments", IEEE Network Operations and Management Symposium, Kyoto, Japan, 1996.

[KOWA96a]   N. Kowalchuk, J. Sholtz, T. Moors, "A Framework for the Management of Networks Based on Information Value", MILCOM'96, USA, 1996.

[KOWA96b]   N. Kowalchuk, P. Blackmore, "Multimedia Services in a Tactical Environment", MILCOM'96, USA, 1996.

[KOWA96c]   N. Kowalchuk, "Research Toward a Military Quality of Service (QoS) Architecture", The Technical Cooperation Program (TTCP) Workshop, 1996.

[KURO93]   J. Kurose, "Open Issues and Challenges in Providing Quality of Service Guarantees in High Speed Networks", ACM Computer Communications Review, Vol 23, No 1, January 1993.

[LAZA96]   A. Lazar, K. Lim, F. Marconcini, " Realizing a Foundation for Programmability of ATM Networks with the Binding Architecture, Journal of Selected Areas in Communications, Sept, 1996.

[LAZA97]   A. Lazar, "Programming Telecommunication Networks", in "Building QoS into Distributed Systems" A. Campbell & K. Nehrstedt (Editors), IFIP, published by Chapman & Hall, 1997.

[LUET98]   J. Luetchford, M. Schreinemachers, N. Morita, H. Arai, "Applications of ATM in Global Networks", IEEE Communications Magazine, August 1998.

[MART97]   J. Martin-Flatin, S. Znaty, "A Simple Topology of Distributed Management Paradigms", Proceedings of Distributed Systems Operations and Management (DSOM) conference, Sydney, Oct. 1997.

[NORT98]   "IP QoS – A Bold New Network", White Paper, Nortel/Bay Networks, 1998, http://www.nortel.com/broadband/IPquality.html

[OLIV98]   H. Oliver, S. Brandt, A. Thomas, N. Charton, "Network Control as a Distributed Object Application", Distributed Systems Engineering, No. 5 (1998), UK.

[P1520]   P1520, "Application Programming Interfaces for Networks", IEEE Draft White Paper, 1998.

[PARK96]   Jong-Tae Park, Su-Ho Ha, "Design and Implementation of CORBA-based TMN SMK System", IEEE Network Operations and Management Symposium, Kyoto, Japan, 1996.

[PAVO98]   J. Pavo, J. Thomas, Y. Bardout, L. Hauw, "Management in the TINA Framework", Communications Magazine, March 1998.

[PORE98]   S. Poretsky, "Connection Precedence and Preemption in Military Asynchronous Transfer Mode (ATM) Networks", MILCOM'98, Boston, USA, 1998.

[RAHK97]   S. Rahkila, S. Stenberg, "Experiences on Building a Distributed Computing Platform Prototype for Telecom Network and Service Management", 5th IFIP Intern. Symposium on Integrated Network Management, USA, 1997.

[RSVP98]   http://www.isi.edu/rsvp/release.html

[SCHM97]   D. Schmidt, A. Gokhale, T. Harrison, G. Parulkar, "A High-Performance End System Architecture for Real-Time CORBA", Communications Magazine, Febr. 1997.

[SHOU99]   P. Shoubridge, M. Kraetzl, D. Ray, "Detection of Abnormal Change in Dynamic Networks", to be presented at *Information, Decision & Control Conference* (IDC'99), Adelaide, March 1999.

[SHAH98]   S. Shah, L. Bowman, R. Riehl, "Mobile and Wireless ATM (WATM) Defence Information Systems Network (DISN)", MILCOM'98, Boston, USA, 1998.

[SHVO98]   W. Shvodian, "Multiple Priority Distributed Round Robin MAC Protocol for Satellite ATM", MILCOM'98, Boston, USA, 1998.

[STAD98]   J.Stadler, J. Gelman, "Performance Enhancement for TCP/IP on Satellite Channel", MILCOM'98, Boston, USA, 1998.

[STIM99]   Phil Stimson, personal communication, March 1999.

[TINA97]   "TINA Consortium delivers software architecture for advanced multimedia networking", TINA-C Press Release, Santiago de Chile, Nov. 1998.

http://www.tinac.com/TINA2000/press/deliver.html

[TINA98]   "TINA – A Common software architecture for multimedia and information services",TINA Consortium, 1998,

http://www.tinac.com/about/nutshell.htm

[UDUP96]   D. Udupa, "Network Management Essentials", McGraw-Hill, New York, 1996.

[VAKI98]   F. Vakil, "A Heuristic for Interoperability Assurance in ATM networks", MILCOM'98, USA, 1998.

[WEBS98]   M. Webster, "Defence Communications Group Overview", CIP Industry Presentation, March 1998.

[WILK97]   D. Wilksch, "Project Parakeet – The performance of Asynchronous Transfer Mode Over Network Trunks", Report DSTO-TR-0551, Communications Division, DSTO, Salisbury, Australia, Nov. 1997.

[YEAD94]   N. Yeadon, F. Garcia, A. Campbell, D. Hutchison, " QoS Adaptation and Flow Filtering in ATM Networks", 2nd International Workshop on Advanced Teleservices and High-Speed Communication Architectures (IWACA '94), Heidelberg, Germany, Sept. 1994.

DISTRIBUTION LIST

Network Control and Management Architectural Framework Supporting Military
Quality of Service

Dr. Marek Kwiatkowski

AUSTRALIA

DEFENCE ORGANISATION

Task sponsor
Director General C3I Development
PD JP 2047 (CWAN)
PD JP 2068 (NOC)
PD JP 2061 (EXC3ITE)

S&T Program
 Chief Defence Scientist
 FAS Science Policy   } shared copy
 AS Science Corporate Management
 Director General Science Policy Development
 Counsellor Defence Science, London (Doc Data Sheet only)
 Counsellor Defence Science, Washington (Doc Data Sheet only)
 Scientific Adviser Policy and Command
 Navy Scientific Adviser (Doc Data Sheet and distribution list only)
 Scientific Adviser - Army (Doc Data Sheet and distribution list only)
 Air Force Scientific Adviser
 Director Trials

 Aeronautical and Maritime Research Laboratory
 Director

 Electronics and Surveillance Research Laboratory
 Director (Doc Data Sheet and distribution list only)

 Chief of Communications Division
 Research Leader Military Information Networks (Dr. M.Flaherty)
 Head Network Architectures (Dr. R. Taylor)
 M. Kwiatkowski (DSTO/CD)
 P. George (DSTO/CD)
 P. Shoubridge (DSTO/CD)
 M. Kraetzl (DSTO/CD)

 DSTO Library and Archives
 Library Fishermens Bend
 Library Maribyrnong
 Library Salisbury (2 copies)
 Australian Archives

Library, MOD, Pyrmont (Doc Data sheet only)

Capability Development Division
Director General Maritime Development (Doc Data Sheet only)
Director General Land Development (Doc Data Sheet only)   Director   General
Aerospace Development (Doc Data Sheet only)
Army
ABCA Standardisation Officer, Puckapunyal, (4 copies)
SO (Science), DJFHQ(L), MILPO Enoggera, Queensland 4051 (Doc Data Sheet
only)
NAPOC QWG Engineer NBCD c/- DENGRS-A, HQ Engineer Centre Liverpool
Military Area, NSW 2174 (Doc Data Sheet only)

Intelligence Program
DGSTA Defence Intelligence Organisation

Director General Information Infrastructure

Director General Corporate Information Policy and Plans

Corporate Support Program (libraries)
OIC TRS, Defence Regional Library, Canberra
Officer in Charge, Document Exchange Centre (DEC) (Doc Data Sheet and
distribution list only)
*US Defence Technical Information Centre, 2 copies
*UK Defence Research Information Center, 2 copies
*Canada Defence Scientific Information Service, 1 copy
*NZ Defence Information Centre, 1 copy

UNIVERSITIES AND COLLEGES

Australian Defence Force Academy
 Library
 Head of Aerospace and Mechanical Engineering
Serials Section (M list), Deakin University Library, Geelong, 3217 (Senior
Librarian, Hargrave Library, Monash University
 Librarian, Flinders University

OTHER ORGANISATIONS

NASA (Canberra)
AGPS
State Library of South Australia
Parliamentary Library, South Australia

OUTSIDE AUSTRALIA

ABSTRACTING AND INFORMATION ORGANISATIONS
Library, Chemical Abstracts Reference Service
Engineering Societies Library, US

Materials Information, Cambridge Scientific Abstracts, US
Documents Librarian, The Center for Research Libraries, US

INFORMATION EXCHANGE AGREEMENT PARTNERS
Acquisitions Unit, Science Reference and Information Service, UK
Library - Exchange Desk, National Institute of Standards and Technology, US

SPARES (7 copies)

Total number of copies: 60

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION DOCUMENT CONTROL DATA	1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE Network Control and Management Architectural Framework Supporting Military Quality of Service	3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION) Document (U) Title (U) Abstract (U)

4. AUTHOR(S) Marek Kwiatkowski	5. CORPORATE AUTHOR Electronics and Surveillance Research Laboratory PO Box 1500 Salisbury SA 5108 Australia

6a. DSTO NUMBER DSTO-TR-0871	6b. AR NUMBER AR-011-074	6c. TYPE OF REPORT Technical Report	7. DOCUMENT DATE September 1999

8. FILE NUMBER E 8709-7-16	9. TASK NUMBER 99/150	10. TASK SPONSOR C3ID	11. NO. OF PAGES 52	12. NO. OF REFERENCES 55

13. URL PDF: http://www.dsto.defence.gov.au/corporate/reports/DSTO-TR-0871.pdf	14. RELEASE AUTHORITY Chief, Communications Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT
Approved for Public Release
OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE CENTRE, DIS NETWORK OFFICE, DEPT OF DEFENCE, CAMPBELL PARK OFFICES, CANBERRA ACT 2600

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CASUAL ANNOUNCEMENT	Yes

18. DEFTEST DESCRIPTORS

Network Control, Network Management, Computer Architecture, Switching Systems, Quality of Service, Military Networks

19. ABSTRACT
The growing demand for multimedia/multiparty services and their rapid design, deployment and modification using cell/packet infrustructure is apparent in the ADF. A well-chosen uniform Military Network Control and Management (M-NC&M) architecture covering both strategic and tactical domains may have an enormous impact on achieving these goals. This report proposes a general framework for such an architecture, in the medium term (5-10 years). The proposed framework follows concepts of an open and programmable network environment, and adds to them military specifics pertinent to the ADF. A particular emphasis of the framework is put on the way the military aspects of Quality of Service should be supported by the M-NC&M.